

Information Resilience Test Against Digital Image Manipulation and Online Media Sending in Steganography Using Least Significant Bit Algorithm

Aditya Aziz Fikri^{✉1} Nur Aynun Siregar² Nurdin³

¹Student in Master of Information Technology Departement, Faculty of Engineering, Malikussaleh University, Bukit Indah, Lhokseumawe, 24355, Indonesia, aditfreedom11@gmail.com

²Student in Master of Information Technology Departement, Faculty of Engineering, Malikussaleh University, Bukit Indah, Lhokseumawe, 24355, Indonesia, nuraynuns@gmail.com

³Master of Information Technology Departement, Faculty of Engineering, Malikussaleh University, Bukit Indah, Lhokseumawe, 24355, Indonesia, nurdin@unimal.ac.id

✉Corresponding Author: aditfreedom11@gmail.com | Phone: +6281362059403

Abstract

Steganography is a method of hiding information, which can be text, images, or videos, in a cover image, secret information is hidden in a way that is invisible to the eye. Steganography is designed to maintain hiding capacity while still considering security and insensitivity to steganalysis. One of the characteristics of steganography is robustness, which can maintain the information in it. So that robustness testing is very important in determining the effectiveness of the steganography algorithm used. This paper aims to test the resilience of information or messages hidden after inserting secret messages in stego images. In this study, the tests carried out include digital image manipulation and the process of sending stego image files. Various types of manipulation such as resizing, compression, and other visual effects. Then it will be explored to assess the extent to which the integrity of the message is maintained. This study resulted in tests carried out related to testing the storage capacity of the cover image greatly affecting each size, the process of sending stego images in PNG format on online media E-Mail, WhatsApp, and Telegram experienced changes in the size of the files received on each platform. However, the file extension does not change, which means there is no file format conversion on the three platforms. In terms of file size, there is a difference in file size on the three online media, but the difference does not affect the extraction of secret messages, which means the message extraction process is 100% successful. The digital image manipulation test carried out, namely crop, resize, brightness, rotate, and flip, most of the tests carried out failed in extracting text messages.

Keywords: steganography, least significant bit, image processing.

Introduction

The development of information technology in the era of globalization has influenced all fields to continue to strive to create better information systems [1]. Any information that exists can be exchanged both secretly and publicly for certain needs via the internet, so it can be said that information is something valuable in this era [2]. However, in reality, information exchanged via the internet is still vulnerable to theft and wiretapping, so a way is needed to secure the data/information that will be sent.

Steganography and cryptography are techniques that are often used in data security, steganography is a method for hiding information, which can be text, images, or videos, in a cover image, secret information is hidden in a way that is invisible to the human eye [3]. Cryptography is the science and art of protecting the security of messages, data, or information through secret writing. The goal is to process information using a specific algorithm, so that the message or information cannot be read or understood by unauthorized parties. In cryptography, there is an Encryption process, which is securing the original message (plain text) into a hidden message (cipher text), and Decryption, which is the process of restoring the encrypted message [4].

The main processes in steganography are embedding and extraction [5], embedding requires a secret message that you want to store and the result is a stego image, the extraction process is the process of restoring the message intact from the stego image. Steganography is designed to maintain the hiding capacity while still considering security and insensitivity to steganalysis [6][7]. One of the characteristics of steganography is robustness, which can maintain the information contained within it [8]. So robustness testing is very important in determining the effectiveness of the steganography algorithm used.

This paper aims to test the resilience of information or messages hidden after the insertion of secret messages in stego

images. In this study, the tests carried out include digital image manipulation and the process of sending stego image files. Various types of manipulation such as resizing, compression, and other visual effects. Then it will be explored to assess the extent to which the integrity of the message is maintained. The results of this study are expected to provide deeper insight into the security and resilience of steganography images in facing possible threats.

Materials & Methods

The framework of the proposed method consists of several phases. First, both the cover image and the secret message will be prepared for the insertion process. Then the message insertion process will be carried out, after the image is inserted, it will be sent via online media such as E-Mail, and several social media to test the extraction of secret messages. After the extraction process is carried out, then the secret message extraction test will be carried out on digital image manipulation such as crop, resize, brightness, rotate, and flip. Figure 1 shows the framework of the proposed method.

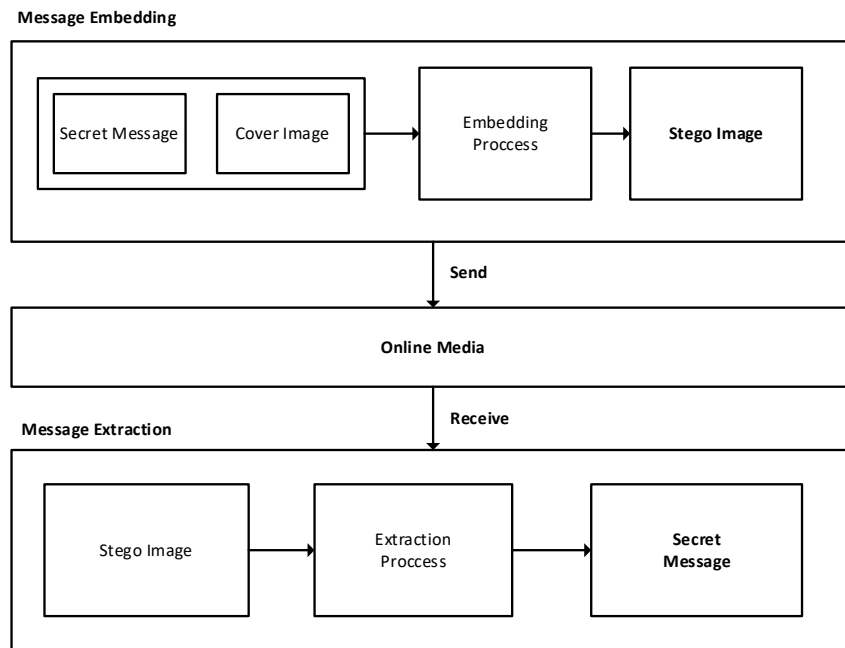


Figure 1. Kerangka Metode Penelitian

Least Significant Bit Algorithm

The algorithm used in this study is the Least Significant Bit (LSB) using the Stego One Bit LSB type, which is a data insertion method that adds information to only one LSB bit in each image pixel [9]. In this process, 8 pixels are needed to insert one character, because each character consists of 8 bits. Only the blue bits are changed, with a value that can be increased or decreased by one on each pixel of the stored image. This method allows the Stego Image to appear to have little change and become smoother after the message is inserted into the Cover Image.

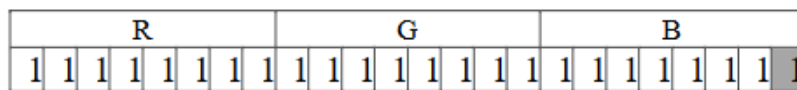


Figure 2. Ilustrasi Stego One Bit LSB

Cover and Stego Image

The cover image used in this study uses a 24-bit RGB image with a PNG file extension, which is a type of lossless compression - compression without losing quality [10], so this type of file is very possible to be used in the future in terms of information exchange on the internet. Then the resulting stego image will be normalized at a size of 900x900 pixels, so a cover image with a ratio of 1:1 is needed so that the results of the stego image can maintain its quality and not invite suspicion from other parties.

Secret Message

Because the stego image produced in this study was normalized to 900x900 pixels, it will produce 810,000 pixels in total [2]. The message storage process is divided into two parts, the first is the process of storing the message length, and the second is the process of storing the secret message. The process of storing the message length is intended to find out the length of the message which will later be extracted the secret message according to the length of the message. The process of inserting both the message length and the secret message will be carried out from the top left pixel to the bottom right sequentially. Each pixel can only store 1 bit, so it takes 8 pixels to store a character, the total number of characters

that can be stored in a 900x900 pixel image can be seen in Function 1.

$$total\ character = \frac{total\ pixel}{8} \tag{1}$$

From Function 1, the total number of characters that can be inserted into the image is 101,250 characters with a binary value of 00011000101110000010₍₂₎, the binary value has 20 bits. Therefore, the length of the text message that can be stored in an image size of 900x900 pixels is 20 pixels. The process of inserting the length of the message starts from pixel (0.0) to (0.19) so that the message that can be stored is 101,247 characters, the calculation of which can be seen in Function 2.

$$secret\ message\ value = \frac{total\ pixel - 20}{8} \tag{2}$$

For example, the message to be inserted is the letter S which has a length of 1 decimal, the value of 1 decimal is 00000000000000000001₍₂₎. Then the binary bit is inserted as much as 20 pixels in the image starting from pixel (0.0) to (0.19) and at pixel (0.20) and so on is the process of inserting message bits. If the inserted message bits exceed the size of the image dimensions, the image cannot be inserted because the message size exceeds the size of the image dimensions.

Resilience Test

This test aims to test the resilience of secret messages that have been inserted into images when secret message extraction is carried out. This test includes several aspects, including testing the amount of message storage, testing delivery on online media, and testing digital image manipulation, such as crop, resize, brightness, rotate, and flip. The results of this test are expected to provide deeper insight into the security of message insertion in digital images and recommendations for future improvements.

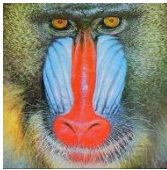

Results and Discussion

In this section, the results of the research conducted will be discussed, including message storage testing, testing on online media, and digital image manipulation testing. The results will be presented in the form of tables in each sub-chapter to facilitate understanding and analysis. In addition, each table will be equipped with an explanation and interpretation of the results obtained, so that readers can understand the impact of various tests on the resilience of secret messages embedded in digital images. This explanation aims to provide a clearer picture of the effectiveness of the steganography method used and the challenges that may be faced in its implementation.

Message Storage Test

In this section, testing is carried out on the amount of secret message storage for the message to be inserted. The cover image sizes used in this test are 900x900, 25x25, 20x10, 10x15, and 10x10. Each cover image size will be evaluated to determine the maximum capacity that can store secret messages without significantly changing the visual quality of the image. The results of this test will provide insight into how effective various image sizes are in accommodating messages, as well as the impact of image size on the integrity and confidentiality of the inserted message. Furthermore, a table will be presented to summarize the test results and an in-depth analysis of the storage capacity of each size.

Table 1. Message storage test

Cover Image	Secret Text	Details
 <p>Baboon.png 512x512 pixel</p>	<p>Lorem, ipsum dolor sit amet consectetur adipiscing elit. Autem voluptate totam in, ullam assumenda molestiae unde officii quasi at nisi vitae? Odio iusto tenetur consequuntur ea odit deserunt modi non animi corporis numquam? Placeat aspernatur et facere a quam id? (266 Characters)</p>	<p>All secret messages has inserted succesfully.</p>
 <p>Boat.png 25x25 pixel</p>	<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fuga voluptatibus atque consequuntur eaque earum accusamus sequi obcaecati beatae qui omnis iusto quos, quam minima, eligendi ea mollitia velit commodi debitis esse veritatis assumenda?</p>	<p>The text message failed to be inserted because the image can only insert 75 characters, the text message entered has 243 characters.</p>

(243 Characters)



Tulips.png
20x10 pixel

Lorem ipsum dolor sit amet
consectetur, adipiscing elit.
(56 Characters)

The text message failed to be inserted
because the image can only insert 22
characters, the text message entered
has 56 characters.



Fruits.png
10x15 pixel

Lorem ipsum dolor sit amet.
(27 Characters)

The text message failed to be inserted
because the image can only insert 16
characters, the text message entered
has 27 characters.



Peppers.png
10x10 pixel

Lorem, ipsum dolor.
(19 Characters)




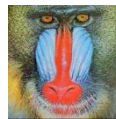






The text message failed to be inserted
because the image can only insert 10
characters, the text message entered
has 19 characters.
















In Table 1 there are 5 results with different dimensional images, the calculation process is obtained using Function 2. In Baboon.png there are 266 characters to be inserted into the image, and all messages can be inserted properly. In the Boat.png image there are 243 characters to be inserted into the image but failed because it exceeds the image size which can only insert 75 characters. In the Tullips.png image there are 57 characters to be inserted into the image but failed because it exceeds the image size which can only insert 22 characters. In the Fruits.png image there are 27 characters to be inserted into the image but failed because it exceeds the image size which can only insert 16 characters. In Peppers.png there are 19 characters to be inserted into the image but failed because it exceeds the image size which can only insert 10 characters.

Online Media Test

In this section, stego image delivery testing is carried out by sending it to online media. The online media that are tested are E-Mail, WhatsApp, and Telegram. The secret message that is carried out for insertion into the cover image uses the sample in Table 1 which is used in Baboon.png to all images, Table 2 is the result of the delivery test on online media.

Table 2. Online Media Test

Send		Receive			Detail
Cover Image	Stego Image	E-Mail	WhatsApp	Telegram	
 Baboon.png 900x900 pixel 622 KB	 Baboon.png 900x900 pixel 600 KB	 Baboon.png 900x900 pixel 586 KB	 Baboon.png 900x900 pixel 586 KB	 Baboon.png 900x900 pixel 600 KB	Message successfully extracted
 Boat.png 512x512 pixel 173 KB	 Boat.png 900x900 pixel 271 KB	 Boat.png 900x900 pixel 265 KB	 Boat.png 900x900 pixel 264 KB	 Boat.png 900x900 pixel 271 KB	Message successfully extracted

					Message successfully extracted	
Tulips.png 768x512 pixel 663 KB	Tulips.png 900x900 pixel 457 KB	Tulips.png 900x900 pixel 446 KB	Tulips.png 900x900 pixel 446 KB	Tulips.png 900x900 pixel 457 KB		
						Message successfully extracted
Fruits.png 512x512 pixel 461KB	Fruits.png 900x900 pixel 429 KB	Fruits.png 900x900 pixel 419 KB	Fruits.png 900x900 pixel 419 KB	Fruits.png 900x900 pixel 429 KB		
						
Peppers.png 512x512 pixel 526 KB	Peppers.png 900x900 pixel 484 KB	Peppers.png 900x900 pixel 473 KB	Peppers.png 900x900 pixel 473 KB	Peppers.png 900x900 pixel 484 KB		

The results of the entire stego image sent to online media did not experience changes in the dimensions of the image. All images sent also did not experience changes in file format, both when sent and received, the file is still in PNG format. In terms of size, each online media received experienced an increase and decrease in file size, only this did not affect the extraction process and the message extraction results were 100% successful on all three online media.

Image Manipulation Test

The testing conducted in this section aims to test the resilience of secret messages when digital image manipulation is carried out. The digital image manipulation process carried out on stego images is in the form of crop, resize, brightness, rotate, and flip. The stego image samples that were tested came from Table 2 in the Baboon.png image, Table 3 shows the results of the crop testing carried out in this study.

Table 3. Crop Testing

Crop	Direction	Details
20%	Left	Message extraction failed
20%	Right	Message extraction success
20%	Top	Message extraction failed
20%	Down	Message extraction success
20%	All	Message extraction failed

Of the five tests conducted, the secret message extraction process in the digital image modification crop testing was only successful in the right and bottom directions, and the rest failed. This was said to have failed because the pixels resulting from the crop test operation hit the pixel area used for inserting the number of messages and the secret message stored. On the other hand, what made the secret message extraction successful was that it did not hit the pixel area of the message storage, but it was not possible for it to fail because the number of messages inserted was still short. Furthermore, Table 4 shows the results of the resize operation carried out in this study.

Table 4. Resize Testing

Resize	Details
10%	Message extraction failed
30%	Message extraction failed
50%	Message extraction failed
70%	Message extraction failed
90%	Message extraction failed
100%	Message extraction failed

The resizing process is carried out gradually by increasing the size gradually from the normal size, but the resize testing results in failure to extract messages at all test sizes. This is because the value of the pixel where the message is stored has changed. The same test was carried out on brightness, a gradual increase in brightness was carried out on the stego image, Table 5 is the result of the brightness testing manipulation test in this study.

Table 5. Brightness Testing

Brightness	Details
10%	Message extraction failed
30%	Message extraction failed
50%	Message extraction failed
70%	Message extraction failed
90%	Message extraction failed
100%	Message extraction failed

The brightness manipulation testing process in this section shows overall failed results. This is caused by changes in pixel values in the image; when the brightness level is increased periodically, the changes significantly affect the pixel values in the image. As a result, the embedded secret message cannot be extracted correctly. This also occurs in Table 6 which presents the results of digital image manipulation testing for the rotate technique.

Table 6. Rotate Testing

Rotasi	Details
CW 90 ⁰	Message extraction failed
CW 180 ⁰	Message extraction failed
CW 270 ⁰	Message extraction failed
CCW 90 ⁰	Message extraction failed
CCW 180 ⁰	Message extraction failed
CCW 270 ⁰	Message extraction failed

In the rotate operation, the entire testing process also failed to extract the secret message where the value of the pixel in the stego image has changed due to image manipulation. Rotation testing is carried out in stages either clockwise or counterclockwise from the normal position. The same results are also obtained in Table 7 by performing the flip operation.

Table 7. Flip Testing

Flip	Details
Horizontal	Message extraction failed
Vertical	Message extraction failed

Conclusions

The tests carried out related to testing the storage capacity of the cover image greatly affect each size, different sizes given as cover images will give different results on the capacity of the message storage. From the process of sending stego images on online media E-Mail, WhatsApp, and Telegram, there is a change in the size of the file received on each platform. However, the file extension does not change which means there is no file format conversion on the three platforms, in terms of file size there is a difference in file size on the three online media, it's just that this difference does not affect the extraction of secret messages which means the message extraction process is 100% successful. In terms of digital image manipulation carried out, only in the 20% cropping process from the bottom and right can the secret message be extracted. It's just that the results obtained will be different if a longer secret message is inserted. The PNG file format is highly recommended in using the LSB algorithm in this study which is resistant to file compression. In terms of image quality produced in the stego image, if viewed with the naked eye there is no change because the LSB algorithm that changes is only the blue channel on each pixel because it uses the Stego One Bit LSB type. However, the drawback of this algorithm is that fewer messages can be stored, but with a dimension size of 900x900 pixels with a number of characters that can be stored as many as 101,247 characters, it is very possible to store a secret text message.

Acknowledgments

Thank you to the organizers of ICOMDEN 2024 who have given the opportunity for this paper to be published. Then thank you to Dr. Nurdin, S.Kom., M.Kom. as the supervisor who has provided direction in writing this paper.

References

- [1] M. Kailani Ridwan, W. Frado Pattipeilohy, and Sanwani, "Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (DCT) Pada Perusahaan Alat Berat," *JURNALILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER*, no. 2, 2020, doi: <https://doi.org/10.33480/jitk.v5i2.1033>.
- [2] A. Aziz Fikhri and Hendrawaty, "Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android," *Jurnal Infomedia*, vol. 3, no. 1, 2018, doi: <http://dx.doi.org/10.30811/jim.v3i1.623>.
- [3] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.
- [4] A. Ikram, I. Warman, and G. Yoga Swara, "Implementasi Algoritma Vigenere Cipher Dan End Of File Pada Steganografi Video," *Jurnal Minfo Polgan*, vol. 12, no. 2, 2023, doi: 10.33395/jmp.v12i2.12418.



- [5] F. Şahin, T. Çevik, and M. Takaoğlu, "Review of the Literature on the Steganography Concept," *Int J Comput Appl*, vol. 183, no. 2, pp. 38–46, May 2021, doi: 10.5120/ijca2021921298.
- [6] Y. Xu, C. Mou, Y. Hu, J. Xie, and J. Zhang, "Robust Invertible Image Steganography," in *CVPR Open Access*, 2022.
- [7] D. Darwis, A. Junaidi, D. A. Shofiana, and Wamiliana, "A New Digital Image Steganography Based on Center Embedded Pixel Positioning," *Cybernetics and Information Technologies*, vol. 21, no. 2, pp. 89–104, Jun. 2021, doi: 10.2478/cait-2021-0021.
- [8] J. Zhang, X. Zhao, and X. He, "Robust JPEG steganography based on the robustness classifier," *EURASIP J Inf Secur*, vol. 2023, no. 1, Dec. 2023, doi: 10.1186/s13635-023-00148-x.
- [9] A. Aziz Fikhri, "Analisis Perbandingan Histogram dan Kualitas Citra Pada Image Steganografi Menggunakan Metode One Bit Least Significant Bit," *Proceeding Seminar Nasional Politeknik Negeri Lhokseumawe*, vol. 2, no. 1, 2018.
- [10] S. Hiremath and A. Shobha Rani, "A Concise Report on Image Types, Image File Format and Noise Model for Image Preprocessing," *International Research Journal of Engineering and Technology*, 2020, [Online]. Available: www.irjet.net