Text to Color Image Steganography Using LSB Technique and XOR Operations

Devi Ratnasari[1], Adam Sekti Aji[2]

[1] *Department of Informatics, Faculty of Information Technology and Electronic Engineering*
University of Technology Yogyakarta, Yogyakarta, Indonesia
[1] deviratnasari@staff.uty.ac.id; [2] adamaji@staff.uty.ac.id

ARTICLE INFO

Article history:
Received June 15, 2019
Revised July 25, 2019
Accepted August 29, 2019

Keywords:
Image Steganography,
Least Significant Bit (LSB),
Text Embedding,
XOR Operation

ABSTRACT

Steganography technique is the art of hiding information in the carrier media to prevent humans from detecting messages or confidential information inside the carrier media. Nowadays steganography has become one of the solutions for information security and confidentiality. This paper applies steganography to hide the text messages into digital color images based on the RGB color model which is also used as a non-secret message. There are two proposed schemes namely the embedding scheme and the extraction scheme by applying the LSB (Least Significant Bit) and triple XOR operation techniques to the binary value of MSB (Most Significant Bit). In addition, a statistical analysis was carried out to measure the quality and difference between the cover image and stego-image by calculating the MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) values.

I. Introduction

In the era of digital communication, the security and confidentiality of information is a domain that is highly considered. Digital information can be exchanged through electronic media and the internet such as files, text messages, images, audio or video. One of the problems that can arise from the internet is data security and privacy. Several methods to overcome this problem have been used such as steganography and cryptography [1][2]. The purpose of the steganography and cryptography is to hide the information. Methodologically steganography is used to hide the confidential information into a carrier image so it will not visually visible using the naked eyes, doesn't cause suspicion and difficult to detect [3].

The LSB (Least Significant Bit) technique is one of the image steganography techniques that is often used in the spatial domain. This technique will hide the secret message bit value into the LSB cover image's bit. Each pixel in the image can be represented in a binary value. There are 8 bits values with $b_7b_6b_5b_4b_3b_2b_1b_0$ arrangement. The $b_7b_6b_5b_4$ are the MSB (Most Significant Bit) and the $b_3b_2b_1b_0$ are the LSB (Least Significant Bit). The MSB bits determine the shape of the object in the image. If the MSB value is changed slightly, it can produce a different image from the original. Meanwhile, if the LSB value is changed, it will not cause significant changes to the shape of the object in the image [4].

The fact that digital data communication through the internet will continue to develop rapidly, so the steganography techniques for information security and confidentiality are also important to be improved. This paper applies the XOR operation to the most significant bits and applies the LSB technique to hide the text messages in 24-bit color cover images.

II. Related Research

Research on secret communications using a lossless steganography approach to hide the text messages into the cover image. This study hides the secret message to prevent the detection of confidential information from other people who do not have access. In this research, the message encryption technique is done by reversing the message strings, replacing each string element with the second advanced string element and rotating the binary value of the message using the generated key. The embedding algorithm used for image steganography is LSB (Least Significant Bit) which hides the bit value of a secret message in the least significant bit of the pixel cover image value [5].

Another study discusses about the concept of image steganography in the spatial domain using LSB (Least Significant Bit) and applied XOR operations. The secret message inserted by performing three XOR operations. First is performed on the 6th and 7th cover images; the second is done on the 8th bit and on the bit of the first XOR operation; the last one is performed on the message bit with the result of the second XOR operation. The results of the operation will replace the last bit value of LSB on the cover image. Experiments have been conducted using grayscale images as the cover images and binary images as secret messages. The secret image and cover image have the same size as 256 * 256 pixels. By using this method, the result of PSNR value is more than 50dB and the MSE value is more than 0.3, while the histogram visualization on the cover image and stego-image shows a distinct pattern difference [2].

Research about image steganography on a spatial domain also has been discussed to hide the text messages into color images. The embedding and extraction process requires a key that is generated randomly in the form of a binary key matrix by referring to the cover image. Embedding and extraction experiments have been successfully carried out using a cover image with a size of 200 × 250 pixels. This study also measure the level of robustness of the proposed technique by comparing the results of the stego-image extraction and the cover image. The result is that it is difficult to recognize or identify the original image and the image which has the inserted secret message [6].

Another study proposed a multi-bits steganography scheme on LSB (Least Significant Bit) to hide the text messages on a personal computer into a color image media. The system allows users to test the steganography technique and choose the best cover image based on the priority of insertion capacity and safety. The capacity of secret messages that can be hidden into the cover image is calculated by adopting insertions on different LSB bits, namely 1, 2, 3 and 4 bits of the cover image. Experiments have been conducted, and show that the maximum success rate of the proposed scheme depends on the secret message data on the cover image used [7].

III. Research Methodology

Two proposed schemes have been conducted, those are embedding data schemes and extraction data schemes. To find out more clearly, the stages can be seen in the sub-section:

A. Embedding Data Scheme

In the embedding data scheme, requires input in the form of RGB color images as the cover image and string as the text message. The length of the text message bit should be equal to or less than the total number of pixel cover images on the RGB channel. The process of hiding text messages in the cover image in this study can be explained in the following steps or can be seen in the visualization in Figure 1:

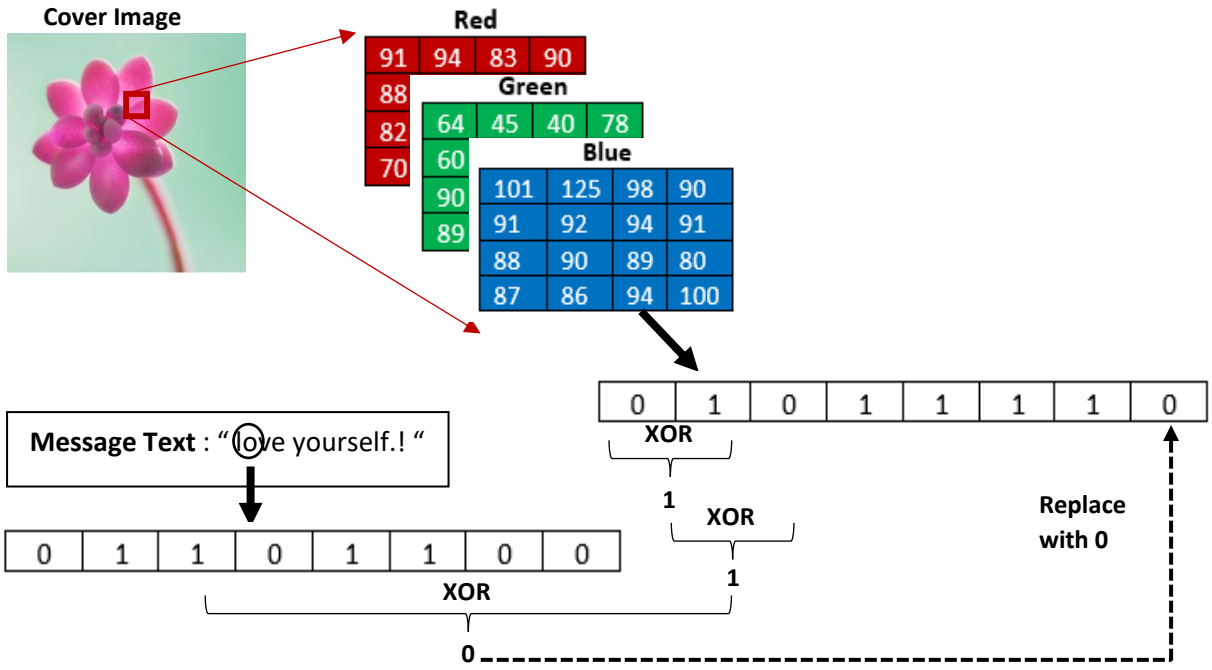

Fig 1. Embedding Scheme

STEP 1: Start
STEP 2: Read and calculate the length of the text message's bit value, and then save as l
STEP 3: Read and count the number of pixels of the cover image in the RGB channel (Red, Green, Blue) by calculating the height and width of the cover image then multiplied by 3 (RGB channel)
STEP 4: Check whether the cover image can hold the bits of the text message using Equation 1.

$$n = \frac{h \times w \times 3}{8} \quad (1)$$

Where: n → the number of messages can hold in the cover image
h → the height of the cover image
w → the width of the cover image
multiplied by the number of 3 because color images consist of three channels namely Red, Green, and Blue channel

STEP 5: If $n > l$ you can continue to the next step
STEP 6: Read the cover image into pixel values for each RGB channels and convert into 8 bit of binary values on each pixel of the RGB channel
STEP 7: Convert the string of the text messages into 8-bit binary values
STEP 8: Perform XOR operation on the 8th bit with the 7th bit
STEP 9: Perform XOR operation on the 6th bit with the results of the XOR operation in step number 8.
STEP 10: Perform XOR operations on the MSB bit (from the results of step number 8) with the text message's bit.
STEP 11: Replace the last of LSB bit of the cover image with the value of the results of the XOR operation in step number 10
STEP 12: Perform step number 8 until step number 11 as many as l value (Text message's bit length)
STEP 13: Save the results and convert it back into a pixel number that will be the pixel value of the stego-image.

B. Extraction Scheme

The extraction phase requires input in the form of stego-image and text message's length value. The output of this phase is the recovered value of the text messages binary. In this study, the extraction scheme of the text messages from a stego-image can be explained in the following steps or can be seen in the visualization in Figure 2.

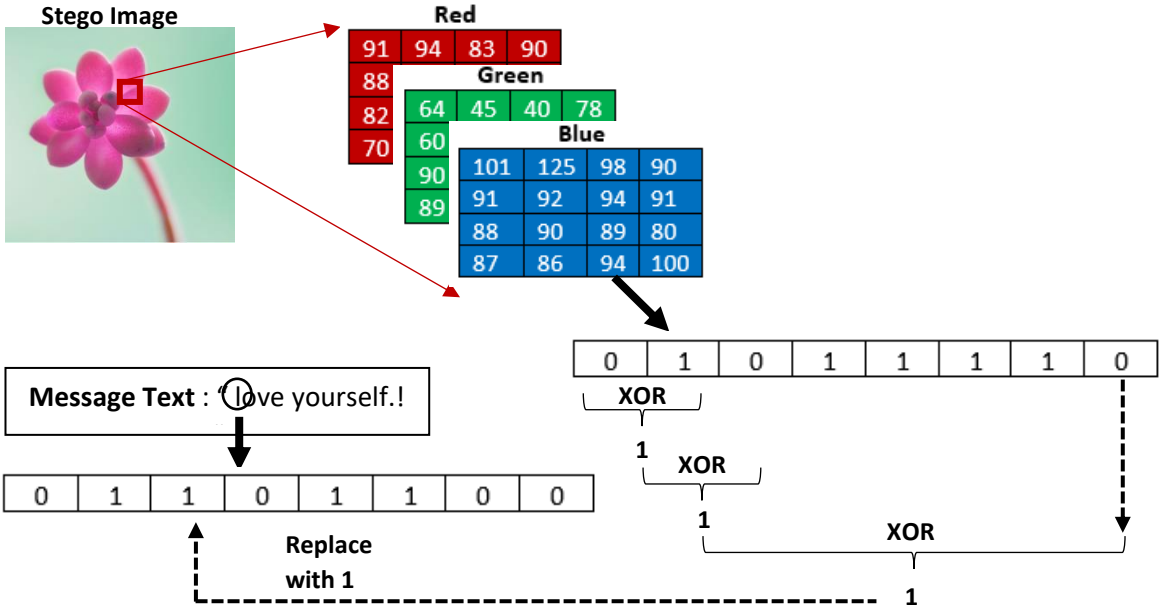

Fig 2. Extraction Scheme

STEP 1: Start

STEP 2: Read the stego-image into pixel values for each RGB channel and convert it into 8-bit binary values on each pixel of the RGB channels.

STEP 3: Perform XOR operation on the 8th bit with the 7th bit.

STEP 4: Perform XOR operation on the 6th bit with the results of the XOR operation in step number 8

STEP 5: Perform XOR operation on the result of step number 4 with the LSB bit (the last bit of the stego-image), then the result will be a text of the message bit

STEP 6: Perform step number 3 until step number 5 as many as *l* value (Text message's bit length)

STEP 7: Save and collect the results of the operation and then convert it into an ASCII number. The results being the recovery value of a text message

IV. Experiment Result And Discussion

In this section, several experiments have been carried out to implement the proposed algorithm. The embedding and extraction scheme simulations have been performed on 24-bit color images of various sizes with the .bmp extension as shown in Figure 3 and Figure 4. The original image and the stego-image also have been analyzed based on the MSE and PSNR values to determine the differences between them. Based on the experimental study, it can be seen that the existence of a secret message on the stego-image generated using the proposed scheme is difficult to detect with the naked eye. Figure 3 shows the cover images.

(a)
Toy.bmp (3264 x 2448)

(b)
Mosque.bmp (767 x 619)

(c)
Cat.bmp (645 x 533)

(d)
Flower.bmp (551 x 451)

(e)
View.bmp (32644 x 2448)

(f)
Sunset.bmp(1632 x 1224)

Fig 3. Covers Image

Figure 4 shows the picture of the stego images with **"love yourself.!"** secret message images.

(a)
Stego_toy.bmp
(3264 x 2448)

(b)
Stego_mosque.bmp
(767 x 619)

(c)
Stego_cat.bmp
(645 x 533)

(d)
Stego_flower.bmp
(551 x 451)

(e)
Stego_view.bmp
(32644 x 2448)

(f)
Stego_sunset.bmp
(1632 x 1224)

Fig 4. Stego images

MSE dan PSNR Analysis

MSE value is the mean square error value between the cover image and the stego-image. MSE and PSNR (Peak Signal Noise Ratio) values are used to measure the difference between the original image and the stego-image [8]. MSE values can be measured using Equation 2.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[C(i,j) - S(i,j) \right]^2 \quad (2)$$

Where: M → cover image or stego-image column
N → cover image or stego image line
C(i,j) → pixel of cover image value at (i, j) position
S(i,j) → pixel of stego image value at (i, j) position

PSNR value is measured in units of dB's and can be calculated using the MSE value as shown in Equation 3.

$$PSNR = 10 \times \log \left(\frac{P^2}{MSE} \right) \quad (3)$$

The P-value is the peak value of the cover image and stego-image, as shown in Equation 4.

$$P = \max \left(C(i,j), S(i,j) \right) \quad (4)$$

The following is Table 1, which shows the results of the statistical analysis calculations of MSE and PSNR values.

Table 1. Statistical Analysis of MSE and PSNR

Images	MSE	PSNR
Toy.bmp	0.0016	62.337
Mosque.bmp	0.0908	56.452
Cat.bmp	0.1102	55.881
Flower.bmp	0.2237	55.459
View.bmp	0.0026	63.738
Sunset.bmp	0.0588	58.148

V. Conclusion

In this paper, we have proposed and described how a combination of the LSB method and XOR operations are used to embed the secret text messages into 24-bit color cover images. The results of applying the embedding scheme have produced a stego-image that is identical to the original image. Stego images are difficult to detect if there is a secret message hidden in the image using the naked eye. Stego image extraction schemes can be used to restore and recover the hidden text message. In addition, by implementing a triple XOR operation on the cover image's bit with the text message's bit provide and improve the embedding mechanism. However, based on the statistical analysis, the algorithms produce a good MSE and PSNR value. The result of PSNR value is more than 55dB and the MSE values are close to 0.

References

[1] D. Ratnasari and H. P. Sejati, "Enkripsi Citra Digital Menggunakan Kombinasi Algoritme Hill Cipher Dan Chaos Map Dengan Penerapan Teknik Selektif Pada Bit Msb," *J. Teknol. Technoscientia*, vol. 10, no. 1, 2017.

[2] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB," in *International Conference on Information and Communications Technology (ICOIACT) Simple*, 2018, pp. 191–195.

[3] A. Anees, A. M. Siddiqui, J. Ahmed, and I. Hussain, "A technique for digital steganography using chaotic maps," *Nonlinear Dyn.*, vol. 75, no. 4, pp. 807–816, 2014.

[4] R. Munir, "Algoritma Enkripsi Citra Digital Dengan Kombinasi Dua Chaos Mao dan Penerapan Teknik Selektif Terhadap Bit-Bit MSB," *Semin. Nas. Apl. Teknol. Inf.*, 2012.

[5] B. Nandi and M. Ghanti, "Hiding Text under Image Cover," no. Icici, pp. 436–441, 2017.

[6] P. Srilakshmi, C. Himabindu, N. Chaitanya, S. V Muralidhar, M. V Sumanth, and K. Vinay, "Text embedding using image steganography in spatial domain," *Int. J. Eng. Technol.*, vol. 7, pp. 1–4, 2018.

[7] A. Gutub and N. Al-juaid, "Multi-bits stego-system for hiding text in multimedia images based on user security priority," *J. Comput. Hardw. Eng.*, vol. 1, no. April, pp. 1–9, 2018.

[8] R. Bhardwaj and V. Sharma, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 832–838, 2016.