File Concealment using the Paillier Method and RGB Intensity Based Steganography

Andysah Putera Utama Siahaan[1*], Leni Marlina[1], Solly Aryza[1], Endrat Fujiyanto[2]
[1]Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Degree Student, Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

Abstract: *Steganography is related to the addition of information to a given medium (referred to as cover media) without making visible changes to it. Most of the proposed steganography techniques cannot be applied to store large-scale data. In the new technique for RGB image steganography, color intensity (R-G-B) is used to determine the number of bits you want to store in each pixel. Meanwhile, to improve the security of stored confidential files, cryptographic methods will be applied. The Paillier cryptosystem invented by Pascal Paillier in 1999 is a probabilistic asymmetric algorithm for public key cryptography. The security of the Paillier algorithm depends on the problem of calculating the n-residue class that is believed to be very difficult to compute. This problem is known as the Composite Residuosity (CR) and is the basis of this Paillier cryptosystem. The software created can save secret files into a digital image into a stego image. The secret file can be extracted out through the extraction process.*

Key Words: *digital image, extraction, confidential, Paillier, RGB, steganography.*

1. INTRODUCTION

Steganography is related to the addition of information to a given medium without making visible changes to it [1]–[3]. The goal is to hide a file attached between the cover media so that the existence of the embedded file becomes hidden. Steganography can be used to hide messages in the image or function as granting patents to the image. Image-based steganography uses the image as a cover medium. Several methods have been introduced for image-based steganography, such as the LSB (Least Significant Bits), Masking and Filtering, Transformations and Spread Spectrum Image Steganography methods, where LSB is one of the simplest methods.

Most of the proposed steganography techniques cannot be applied to store large-scale data. Steganography techniques for new RGB imagery are presented in the paper "RGB Intensity Based Variables-Bits Image Steganography" [4]. In the new technique for RGB image steganography, color intensity (R-G-B) is used to determine the number of bits you want to store in each pixel. Channels that consist of low color values can store larger amounts of data bits. Rows of channels are chosen randomly based on a key that is shared. This technique guarantees a minimum capacity and can accommodate it to store extensive data [5]. The algorithm developers claim that the algorithm has better performance than the previous algorithm. This algorithm can also be used to store different numbers of bits per channel, but still can provide very high capacity for the cover media . Meanwhile, cryptography allows people to leave secret messages found in the physical world into the electronic world, thus enabling people to do business electronically without doubts about forgery, theft, and fraud. Every day hundreds of thousands of people interact electronically, whether through e-mail, e-commerce, ATMs or cell phones. Increased information dissemination electronically has resulted in increased dependence on cryptography. One of the roles of cryptography is to do data security by using cryptographic algorithms. The Paillier cryptosystem invented by Pascal Paillier in 1999 is a probabilistic asymmetric algorithm for public key cryptography. With probabilistic encryption, a cryptanalyst can no longer encrypt random plaintexts to find the correct ciphertext. This Paillier algorithm is a probabilistic encryption algorithm that is more efficient because of the process of encryption per character and not per bit. This combination of cryptographic methods and steganography will produce a system with a very high level of security.

2. METHODOLOGY

2.1 Paillier Method

Merging cryptography with steganography is a good thing. Cryptography will increase data security [6]–[8] The Paillier Cryptosystem discovered by Pascal Paillier in 1999 was a probabilistic asymmetric algorithm for public key cryptography [9]. The problem of calculating n-residue classes is believed to be very difficult to compute. This problem is known as the Composite Residuosity (CR) and is the basis of this Paillier cryptosystem. This scheme is an additively homomorphic cryptosystem, which means that given the public key and encryption of m1 and m2, one will be able to calculate the encryption of m1 + m2. As with the RSA algorithm, a value of n = p.q is needed where p and q are large primes. Besides that, it is also necessary to declare the Totient function from Euler, $\phi(n) = (p - 1)(q - 1)$ and Carmichael function, $\lambda(n) = \text{lcm}(p - 1, q - 1)$.

Assume | $\mathbb{Z}_{n^2}^*$ | = $\phi(n^2) = n\phi(n)$ then for all w ∈ b$\mathbb{Z}_{n^2}^*$ ı :

$$w^{\lambda} = 1 \bmod n$$
$$w^{n\lambda} = 1 \bmod n^2$$

This theorem is called the Carmichael theorem. Whereas, a z number is said to be the n modulo residue of n2 if there is a number y ∈ such that:

$$z = y^n \bmod n^2$$

This theorem is known as the Composite Residuosity (CR) theorem which is the basis of the Paillier algorithm. Meanwhile, if a set of Sn = {u <n2 | is taken u = 1 mod n} which is a multiplication subgroup of integer modulo n2 through an L function, then the following equation:

$$\forall u \in S_n \qquad L(u) = (u - 1) / n$$

2.2 Partition Scheme

In this algorithm, a partitioning scheme is defined as a series of decreasing monotone [ai], i = 1 to 8. Assume the color value of a channel is c. Then the channel with the value c stores the data bit if c> = ai, and for all j, j <i, c <aj. In order for the algorithm to run correctly, only a valid partitioning scheme is used. A valid partitioning scheme can be defined as follows. Suppose [ai] is a partitioning scheme where i the lower bits of ai are all valued 0. Assume [bi], i = 1 to 8, is another row, where bi is produced by changing all values from lower bits of i from ai to 1. If ai> bi + 1, i = 1 to 7, then [ai] is a valid partitioning scheme. This simple condition ensures that the number of data bits read from a channel on the receiving side is the same as that stored on the sending side [10]–[12].

2.3 RGB Intensity Based Steganography Algorithm

The idea behind this algorithm is that for insignificant colors, the number of bits that can be changed significantly per channel can be more than an RGB image [13]. The idea of this algorithm is that the lower color values of a channel have a smaller effect on the overall color of the pixel than the higher color values. Therefore, more bits can be changed in a channel that has a 'low' value than a channel that has a 'high' value. Thus, this algorithm can be described as follows:

1. Use one of the three channels as an indicator. A row of indicators can be made random, based on a key that is used together between the sender and receiver.

2. Data is stored in one of two channels other than indicators. Channels with the lowest color values between two channels other than the indicator will store the data at least significant bits.
3. The number of bits to be stored depends on the color value of the channel. The lower the color value, the more data bits can be stored. Therefore, it takes a partition of the color value. Through experiments carried out by the algorithm developer, it is known that the optimal separation depends on the cover image used.
4. It is necessary to know which channel stores data bits to restore data. It can be done by looking at the least significant bits of both channels besides the indicators:
5. If the bits are the same, then the channel that follows the indicator in the cyclic sequence stores the data.
6. If the bit is not the same, the channel that precedes the indicator in the cyclic sequence that stores data.

The Paillier method is a probabilistic asymmetric algorithm for public key cryptography. This Paillier method uses the concept of the problem of calculating n-residue class known as the Composite Residuosity (CR). RGB image steganography is a concept to insert a data into the image so that the data information is hidden and only the right party can extract the information out. In the work process of RGB image steganography, there are two processes, namely the encoding process and the decoding process. The following figure shows the encoding process on the sending side of the flowchart form. It should be noted that it is assumed that the shared key and partitioning scheme have been agreed between the two parties. After all, processes are complete, header information that contains the number of pixels will be inserted.

3. RESULT AND DISCUSSION

Test results in the form of an implementation of a program that has been made using a programming language. To use this software, the program will run. The main view of the program is shown in the following picture.

3.1 Embedding

The 'Message Insertion' link is used to do the message insertion process. The 'Message Insertion' form can be seen in the following figure.

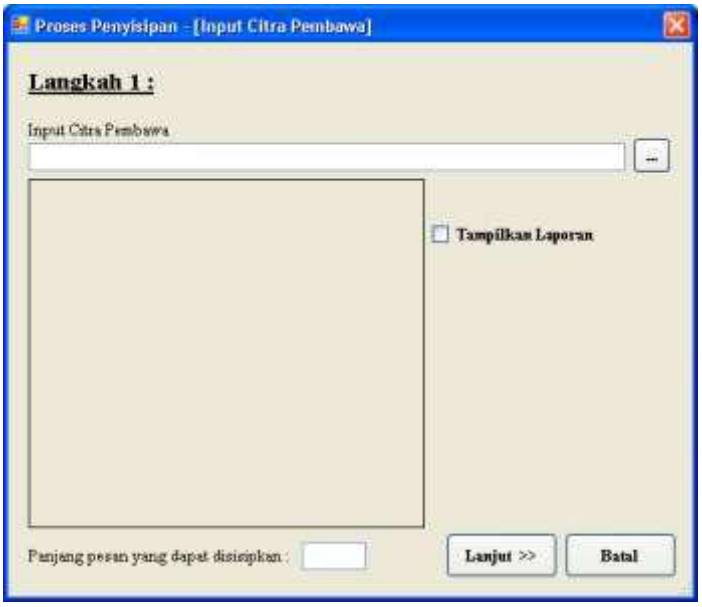

Figure 1. Message Insertion Form Display

Select the image that will be used to store confidential message data. Choose the desired image file. After that, click the 'Open' button. Meanwhile, to cancel the image file selection process, click the 'Cancel' button. Display the Paste Secret Message form can be seen in the following picture.

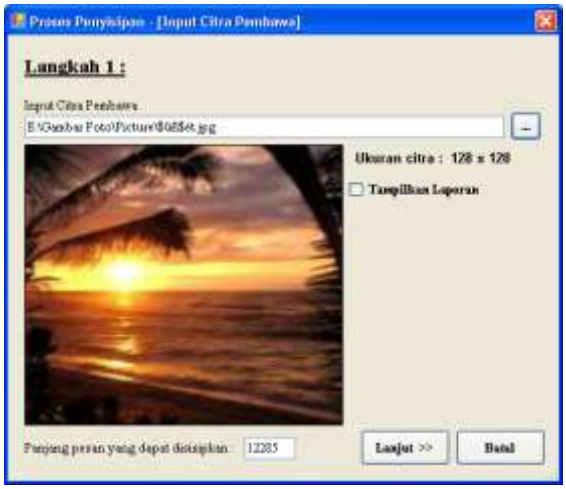

Figure 2. Paste Display of Secret Messages After Data Input

After all, data has been entered, click the 'Continue >>>' link so that the system will display the next step of the insertion process, which is the process of filling in the secret message and encryption. The system view can be seen in the following figure.

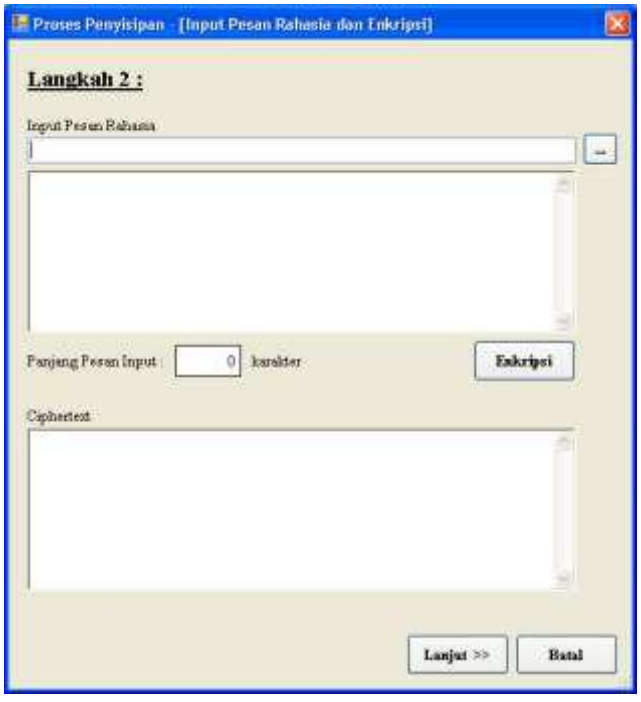

Figure 3. Input Display of Secret Message

Select the secret message file that will be inserted into the cover image. To open the Open dialog box for selecting secret message files, click the link '... '. The Open dialog box can be seen in the following picture.

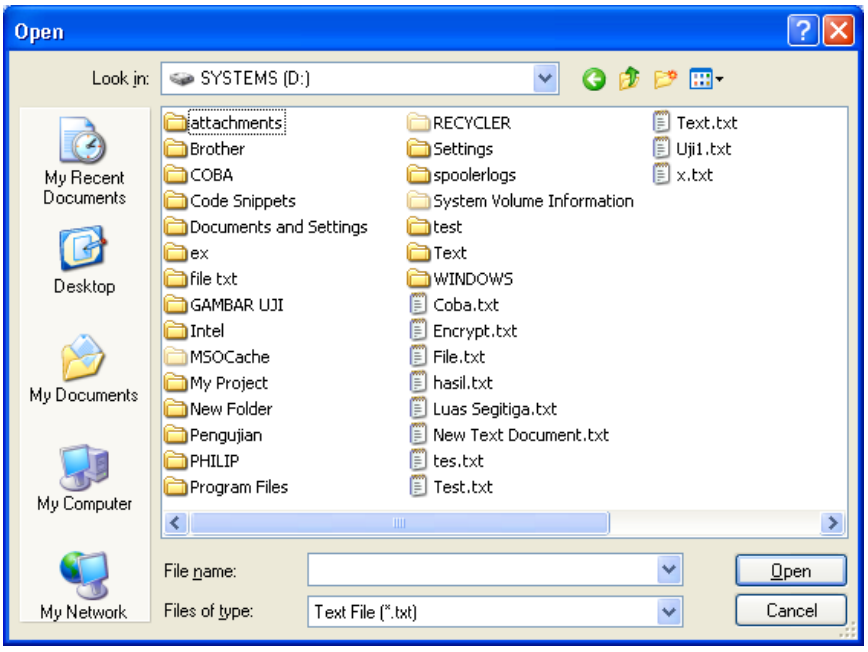

Figure 4. Display of the Open Dialog Box for Secret Message Files

Select the desired secret message file. After that, click the 'Open' button. Meanwhile, to cancel the image file selection process, click the 'Cancel' button. The Secret Message Input form view can be seen in the following picture.

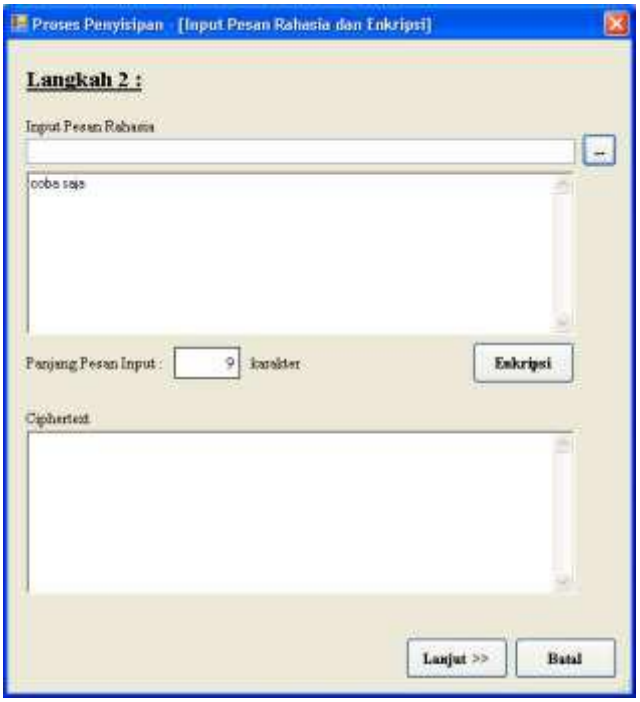

Figure 5. Input Form Display Secret Message After Input

After that, click the 'Encryption' button to encrypt the secret message entered so that the system will encrypt the secret message and display the ciphertext results obtained. The Secret Message Input form will look like the following picture.

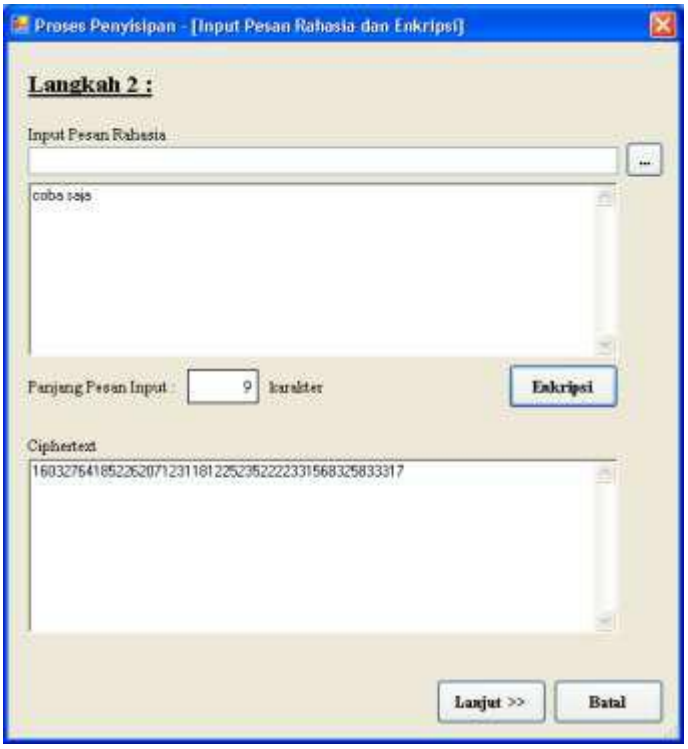

Figure 6. Input Form Display Secret Message After Encryption

After that, click the 'Continue' button so the system will show the process of pasting the secret message to the cover image. The form display Paste Ciphertext to Carrier Image can be seen in the following figure.

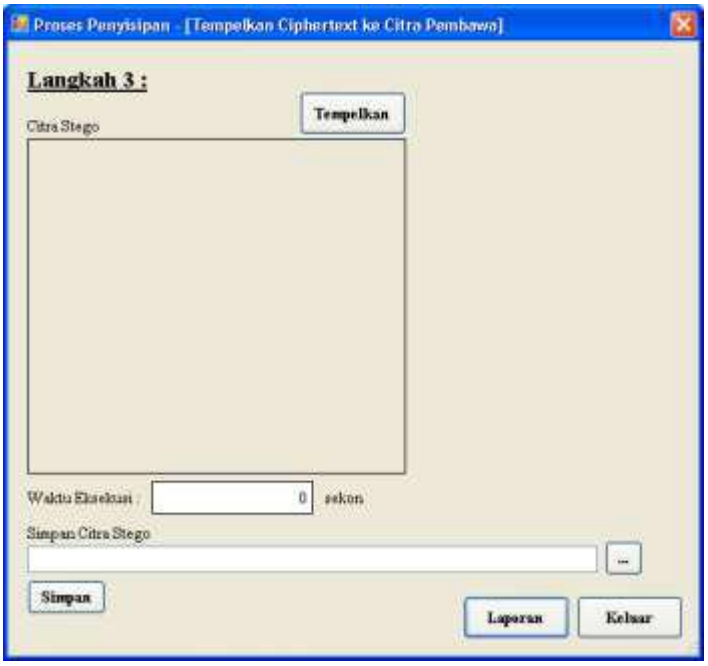

Figure 7. Display Form Paste Ciphertext into Carrier Image

Click the 'Paste' button to make the process of inserting a secret message into the cover image. Display form Paste Ciphertext to Image Carrier after the attachment process can be seen in the following figure.

Figure 8. Display Form Attach Ciphertext to Carrier Image

3.2 Extraction

The 'Extraction' link is used to extract the secret message from the stego image media. The Secret Message Extraction form display can be seen in the following picture. Click the 'Open' link to select the steganographic image file to extract from the secret message. After that, click the 'Extraction' button to extract the ciphertext from the stego image. The appearance of the form after the extraction process can be seen in the following figure.

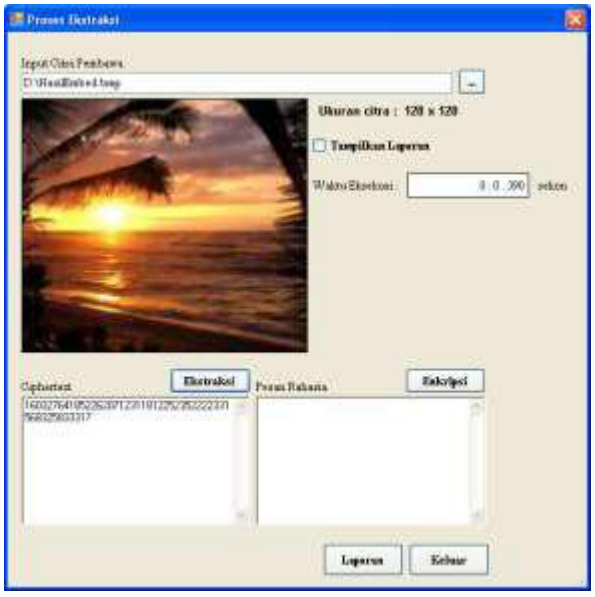

Figure 9. Display of Secret Message Extraction Form After Extraction Process

After that, click the decryption button to make the decryption process of the ciphertext obtained. After completing the extraction process of the secret message, the display of the Secret Message Extraction form will look like the following picture.

Figure 10. Display of Secret Message Extraction Form After Message Decryption Process

3.3 Comparison

The 'Comparison Results' link is used to display the comparison process between two images using the MSE formula. The 'Comparison' form display can be seen in the following picture. Choose the first and second image files to be compared. After that, click the 'Process' button so the system will display the results of the comparison, as shown in the following image.

Figure 11. Display of Comparison After Process Results

4. CONCLUSION

After completing the creation of this software, the author can draw some conclusions as follows. Based on the test results, there does not appear to be a difference between the original image and the stego image in plain view. It s can be seen in the relatively small MSE value, where the smaller the MSE value between two

digital images means that the two images are more similar. The process of changing/deleting certain parts of the image does not have an impact on the inserted message, with the possibility of changes to the message content is relatively small.

REFERENCES:

1. A. P. U. Siahaan, "Noise-Like Region Security Improvisation in BPCS Steganography."
2. R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, pp. 1–5, 2018.
3. A. P. U. Siahaan, "High Complexity Bit-Plane Security Enchancement in BPCS Steganography," *Int. J. Comput. Appl.*, vol. 148, no. 3, pp. 17–22, 2016.
4. M. T. Parvez and A. A.-A. Gutub, "RGB Intensity Based Variable-Bits Image Steganography," in *2008 IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 1322–1327.
5. W. Stallings, *Cryptography and Network Security Principles and Practices*, 4th ed. Prentice Hall, 2005.
6. A. P. U. Siahaan, *How to Code: Advanced Encryption Standard in C#*. Medan: Fakultas Ekonomi Universitas Panca Budi, 2018.
7. A. P. U. Siahaan, "Rail Fence Cryptography in Securing Information."
8. A. P. U. Siahaan, "Securing Short Message ServiceUsing Vernam Cipher in Android Operating System," *IOSR*, Apr. 2016.
9. P. Paillier and D. Pointcheval, "Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries," 1999, pp. 165–179.
10. R. Lanfear, B. Calcott, D. Kainer, C. Mayer, and A. Stamatakis, "Selecting optimal partitioning schemes for phylogenomic datasets," *BMC Evol. Biol.*, vol. 14, no. 1, p. 82, 2014.
11. A. Putera Utama Siahaan, E. Elviwani, and B. Oktaviana, "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," in *Proceedings of the Joint Workshop KO2PI and The 1st International Conference on Advance & Scientific Innovation*, 2018.
12. A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption."
13. S. Prasad and A. K. Pal, "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing," *R. Soc. Open Sci.*, vol. 4, no. 4, p. 161066, Apr. 2017.