Analysis Stego-Image Extraction Using ROT13 and Least Significant Bit (LSB) Algorithm Method on Text Security

Hillman Akhyar D[1], Merry Anggraeni[2], Tomi Defisa[3]

[123]Jurusan Sistem Informasi, Universitas Budi Luhur
[1]Jl. Ciledug Raya, Jakarta Selatan, 12260
e-mail : [1]hillmanakhyardamanik@gmail.com, [2]merryanggraeni1230@gmail.com,
[3]tomidefisa@gmail.com

ABSTRACT

Cryptography is both a science and an art to keep the message confidential. While steganography is the science and art of hiding secret messages in other messages so that the existence of such secret messages is unknowable and generally serves to disguise the existence of confidential data making it difficult to detect and protect the copyright of a product. Steganography requires two properties, namely container media and secret messages. The application of steganographic and cryptographic combination is done by Least Significant Bit (LSB) and ROT13 algorithm. Steganography with the LSB method is one of the methods used to hide messages on digital media by inserting it to the lowest bits or the most right bits of the pixel data that compile the file. In this research, the authors propose the technique of securing Steganography secret messages with layered security, by adding Cryptography to secret messages that will be inserted into digital images and then messages inserted into digital images through Steganography using LSB method.

Keywords: ***Steganography, Least Significant Bit, Cryptography , ROT13***

1. PENDAHULUAN

The security factor is an important thing when communicating on the internet network. Many cases of information leaks that occur when communicating via the Internet network. One method for securing a secret message is Steganography. As the study of Steganography techniques develops, various methods are used to insert secret messages into images using Steganography. One well-known method is the Least Significant Bit (LSB) because the method is simple enough to hide a secret message that has been converted into binary by inserting it in the last pixel that compiles the file. Some applications use this technique and can be used freely by downloading it from the internet are OpenStego and Silent Eyes. With more populer and widely used, need additional security on Steganography so that if the secret message is successfully extracted by unwanted parties, the message still cannot be revealed.

Various cryptographic techniques that have been widely used so that the source code to solve many scattered in several internet sites. Therefore we need a layered and unique Cryptography for secret messages to be random. In this way it is expected that the message will be delivered more secure security and not easily revealed by users who try to steal information.

2. THEORETICAL BASIS AND THE CONCEPT FRAMEWORK

2.1 Steganography

Steganography is the art and science of writing hidden messages or hiding messages in such a way that in addition to the sender and receiver, no one knows or realizes that there is a secret message [6]. With Steganography then the owner of the data can hide the copyright information such as the creator's identity, the date created, until the message to a desired person. Steganography hide information into various types of data such as: images, audio, video, text or binary files.

Steganography method in such a way in hiding the contents of a data in a media cover or other digital data that is not expected by ordinary people so as not to arouse suspicion to the person who saw it. The advantage of steganography compared to cryptography is that the messages sent do not attract attention so that the container medium that carries the message does not arouse suspicion for a third party. To extract hidden messages. These processes can be seen in the picture below:

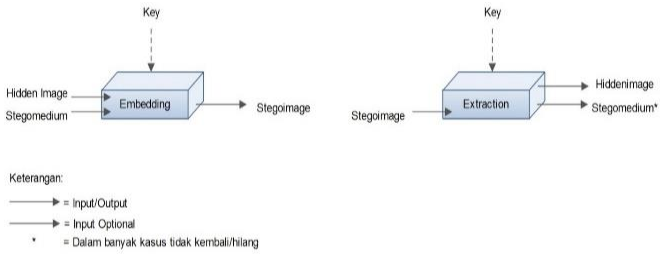

Figure 1 Message concealment process

Figure 1 shows the process of concealment of messages where in the first part, the process of embedding hidden image that would be hidden secretly into Stegomedium as a storage medium, by entering a specific key (key), so generated media with hidden data in it (stegoimage). In Figure 2, execute the extraction process on the stegoimage by entering the same key so as to recover the hidden image. Later in most steganographic techniques, message extraction will not restore the initial stegomedium exactly the same as stegomedium after extraction has even largely lost. Because when the message storage is not done the initial conditions record of stegomedium used to store the message (Cox et al, 2008). In making Steganography there are three things to note [7], namely: 1) Fidelity 2) Recovery 3) Robustness.

2.2 Least Significant Bit

In Least Significant Bit Algorithm, both the data and the image to be used as cover object are converted from their pixel format to binary. And the Least Significant Bit of the image is substituted with the bit of the data to be transferred so as to reflect the message that needs to be hidden. The bits of the data replace each of the colors of the Least Significant Bit of the Image.

Table 1 Showing 3 Letters With Ascii Values and Corresponding Binary Values

No.	Letter	ASCII Values	Binary Values
1	A	65	01000001
2	M	77	01001101
3	I	73	01001001

To hide AMI with the Binary Code (01000001 01001101 01001001) using Least Significant Bit Algorithm, each bit with the least significant bit of each color that made up the Pixel is flipped. LSB method is a method used to hide a message by way of paste at low bit or bits of the rightmost pixel data compiled on the file. In 24 bit bitmap images, each pixel (dot) in the image consists of three color arrangements, red, green and blue (RGB) each composed by an 8 bit (byte) number from 0 to 255 or with binary format 00000000 Until 11111111. Thus, in each 24 bit bitmap image pixel we can insert 3 bits of data. The disadvantage of this LSB method is that it can drastically change the color element of the pixel if it is not correct in replacing the bits or the inserted message is too long. So it can show the real difference from the original image with the picture that has been inserted message. While the advantages of the LSB method is the algorithm used quickly and easily.

Since the bits that are replaced are low bits, then the change only changes the byte value one higher or one lower than the previous value. Suppose the byte represents a red color, so changing one LSB bit does not change the red color significantly. After all, the human eye cannot distinguish small changes. Let's say the image data segment before the change:

00110011 10100010 11100010
The data to be hidden is '1 1 1'.
Image data segment after '1 1 1' is hidden:
00110010 10100011 11100011

The size of the data to be hidden depends on the size of the container image. In 24 bit images of 256x256 pixels there are 65536 pixels, each pixel measuring 3 bytes (RGB component), means that there are 65536x3 = 196608 bytes in whole. Since each byte can only hide one bit in its LSB, the size of the data to be hidden in the maximum image is: 196608/8 = 24576 bytes. The larger the data is hidden in the image, the greater the likelihood that the data is corrupted by manipulation in the container image.

2.3 Cryptography

Cryptography is a science that studies how to keep data or messages safe when sent, from the sender to the recipient without interference from third parties. The word Cryptography [8] comes from the Greek word "krypto's" which means hidden and "graphein" which means writing. So the word Cryptography can be defined as the phrase "hidden writing". According to Request for Comments (RFC), Cryptography is a mathematical science that deals with

the transformation of data to make its meaning incomprehensible (to hide its meaning), to prevent it from unauthorized change, or to prevent it from unauthorized use. According to Bruce Scheiner, written in his book Applied Cryptography, there are four fundamental purposes of the science of cryptography is also an aspect of information security that is: 1). Confidentiality 2) Integrity 3) Authentication 4) Non repudiation

2.4 ROT13

ROT13 is a method of encryption algorithm similar to Caesar Chiper which is only seen from its length alone, ie: Rotate by 13, at a glance it is predictable that ROT13 is a cryptographic method using a 13-step shift (k = 13). In this system a letter is replaced with a letter that lies 13 positions from it.

Table 2 System Replace Letter in Rot13

A/a	B/b	C/c	D/d	E/e	F/f	G/g	H/h	I/i	J/j	K/k	L/l	M/m
⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
N/n	O/o	P/p	Q/q	R/r	S/s	T/t	U/u	V/v	W/w	X/x	Y/y	Z/z

For example, the letter "A" is replaced with the letter "N", the letter "B" is replaced with the letter "O", and so on. This encryption is the use of the Caesar's password with a slide 13. ROT13 is usually used on internet forums, so spoilers, puzzle answers, dirty words, and the like are not read at a glance.
Mathematically, this can be written as: C ROT13 = (M) To return back to its original form ROT13 encryption process twice.
M = ROT13 (ROT13 (M))

2.5 Related Works

The review of the study used as a reference in conducting this research refers to some related studies that have been done before. Several works have been done regarding information hiding trough text steganography. Some researcher conducted a survey on two security tools- cryptography and steganography. Designed the application of steganography using Least Significant Bit (LSB) in which the previous message is encrypted using the Advanced Encryption Standard algorithm (AES) and it can restore the previously hidden data [1]. In this paper, a hybrid technique is introduced by combining the cryptography and Steganography properties. Also for data encryption vary the block size in place of fixed block[2]. Secured model has been developed by combining cryptographic and Steganographic security. Sequential algorithm is used for Steganography and Symmetric XOR algorithm is used for Cryptography[3]. Applying Rotor Caesar cipher on the message followed by 2 bit LSB Steganography[4]. Embedding the secret message into the cover text the stego-text is transmitted over the unsecured communication channel[5].

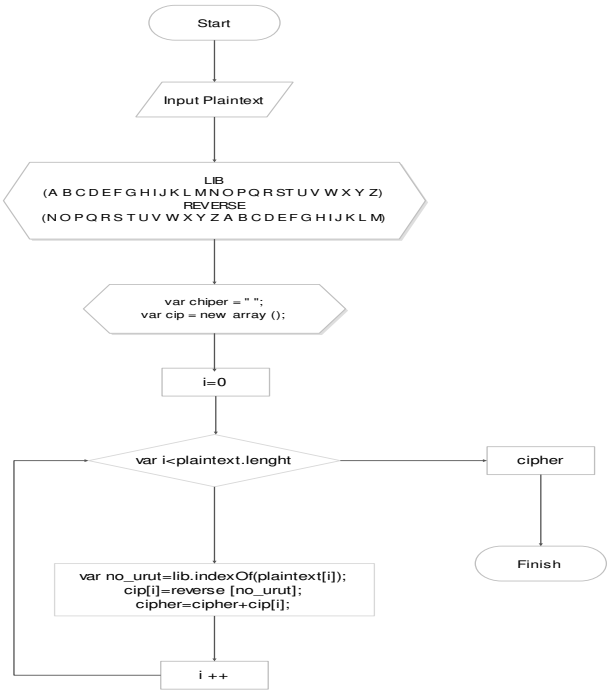

Figure 2 Algoritma of ROT13 in System

Furthermore, the implementation of stegano with LSB method

2.6 LSB Algorithm

If the LSB of the pixel value of cover image C(i,j) is equal to the message bit SM of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to SM.

message embedding Procedure is given below:

S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and SM = 0

S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and SM = 1

S(I,j) = C(i,j), if LSB(C(i,j)) = SM

Where LSB (C(i, j)) stands for the LSB of cover image

C(i,j) and "SM" is the next message bit to be embedded

S(i,j) is the stego image.

2.7 Prototype Testing Model

In this research, system testing or testing of test equipment is done by qualitative and quantitative method. Qualitative method by testing the testers with various types of images as cover image and various types of characters as a secret message to be inserted. With it can know the level of success of research conducted.

2.8 Strategic Plan

Aspects of the system in this study include the system used for the implementation of test equipment. This system is used by senders of secret messages as well as recipients of secret messages utilizing Steganography. The system used is a computer equipped with a network to exchange confidential messages.

3. IMPLEMENTATION AND TESTING OF STEGANOGRAPHIC SYSTEMS

1. Interface Design

Interface Design is a user communication tool with software created.

Figure 3 Home Page Process Embedding and Extractions

From Figure 3. it can be seen that inside the main page there are four buttons. The buttons are Cover Image button, Text Message embedding, Stego-Image and Text extract. The embedding button is used to start the insertion process, the extraction key is used to start the extracting process. Next comes the ROT13 column which is useful as a result.

- Embedding process

  Embedding Button is the process of uploading file cover image selection and insertion of text messages. On this Embedding Button the user or sender of the message will input a message to be sent to the recipient of the message and also select the cover image that matches the length of the message character.

  Data Embedding Algorithm

  Step 1: Extract the pixels of the cover image.
  Step 2: Extract the characters of the text le.
  Step 3: Extract the characters from the Stego key.
  Step 4: Choose first pixel and pick characters of the Stego key and place it in first component of pixel.
  Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.
  Step 6: Insert characters of text le in each rst component of next pixels by replacing it.
  Step 7: Repeat step 6 till all the characters has been embedded.

- Extraction

  Data Extraction Algorithm

  Step 1: Extract the pixels of the stego-image.
  Step 2: Now, start from first pixel and extract stego key characters from first component of the

pixels. Follow Step3 :Up to terminating symbol, otherwise follow step 4.
Step 4: If this extracted key matches with the key entered by the receiver, then follow step 5, otherwise terminate the program.
Step 5: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.
Step 6: Extract secret message.
component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.

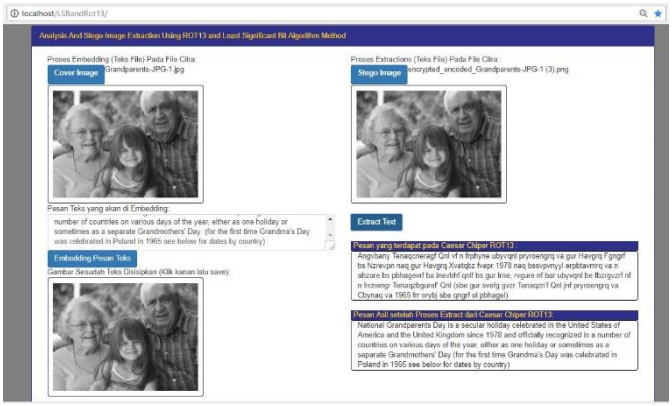

Figure 4 Graphical Interface Design of Extraction Message

2. Testing System

System testing is done to prove that the data security system developed can improve the security and confidentiality of messages sent. Tests were conducted on LSB through two types of testing. First, LSB was tested against Fidelity, robustness, and recovery. Second, LSB is tested through the Frhed program to find out which bit positions are changing on the cover-data. Testing Against Steganograpi Criteria:

Figure 5 Cover-Image-NASA image file view before and after message inserted

Another test for cover quality before and after the message inserted can be seen in the table III below:

Table 3 Table Viewing Image File Cover-Nasa Before and After The Message Inserted

Name Cover Image	Data Cover Resolution	Character Inserted	Type Data Cover
Grandparents-JPG-1	556x143	126	JPG
Name Stego Image	**Data Cover Resolution**		
encrypted_encoded_Grandparents	556x143		

From some tests that have been done seen that the cover image with stego-image that has contained text messages visible is not visible at all and no visible difference at all and also the image dimension before and after the inserted message does not change. This is due to changes in the diagonal bytes of the red component on the cover image will only result in changes of some bytes higher or lower, the change will not display any significant changes in the stego-image. Thus the Lest Significant Bit (LSB) method has met the aspect of imperceptibility as one of the criteria of a good steganographic algorithm. The following summary results in the process of testing the quality of image file cover before and after the message inserted can be seen in the table IV below:

Table 4 Testing Image File Before and After Message Inserted

No.	Name Cover Image	Type Cover Data	Data Cover Size	Data Cover Resolution	Character Length	Image JPG
1	Taj Mahal	JPG	90.7KB	800x533	63 Word	
	Name Stego Image	**Type Cover Data**	**Data Cover Size**	**Data Cover Resolution**		
	encrypted_encoded_Taj Mahal	PNG	1.22MB	800x533		
2	**Name Cover Image**	**Type Cover Data**	**Data Cover Size**	**Data Cover Resolution**	126 Word	
	Grandparents-JPG-1	JPG	59.0KB	556x143		
	Name Stego Image	**Type Cover Data**	**Data Cover Size**	**Data Cover Resolution**		
	encrypted_encoded_Grandparents	PNG	674KB	556x143		
3	**Name Cover Image**	**Type Cover Data**	**Data Cover Size**	**Data Cover Resolution**	281 Word	
	CloudyGoldenGate_grayscale	JPG	94.4KB	500x384		
	Name Stego Image	**Type Cover Data**	**Data Cover Size**	**Data Cover Resolution**		
	encrypted_enco_CloudyGoldenGate	PNG	563KB	500x384		
4	**Name Cover Image**	**Type Cover Data**	**Data Cover Size**	**Data Cover Resolution**	465 Word	
	Flower	JPG	963KB	480x361		
	Name Stego Image	**Type Cover Data**	**Data Cover Size**	**Data Cover Resolution**		
	encrypted_encoded_Flower	PNG	963KB	480x361		

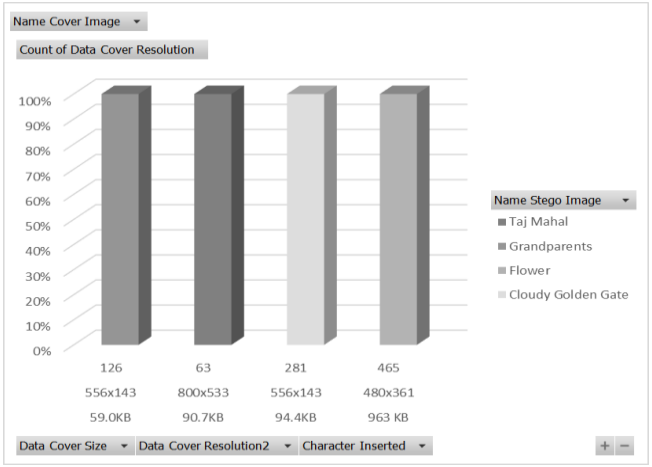

Figure 6 Graphic of Testing image file before and after message inserted

From some tests performed it can be seen that the extraction results from the stego-image produce plaintext corresponding to the plaintext sent by the previous sender in the embedding process. Thus, the Least Significant Bit (LSB) algorithm used in this research has fulfilled the recovery aspect. Steganographic image byte change is performed using an additional application. The Fhred application will read the image file and display the image bytes in hexadecimal form. To facilitate the proof, then the changes that occur in steganographic images can not be seen just by the eye. Therefore, the proof of bitmap image on each cover image above will be translated with Hexadecimal Editor application.

Table 5 Cover and Stego Image in Hexadecimal Dump

No.	Name Cover Image	Jenis Cover Data	Ukuran Cover Data	Resolusi Cover Data	Panjang Karakter	Image JPG
1	Taj Mahal	JPG	90.7KB	800x533	63 Word	
	Name Stego Image	**Jenis Cover Data**	**Ukuran Cover Data**	**Resolusi Cover Data**		
	encrypted_encoded_Taj Mahal	PNG	1.22MB	800x533		
2	**Name Cover Image**	**Jenis Cover Data**	**Ukuran Cover Data**	**Resolusi Cover Data**	126 Word	
	Grandparents-JPG-1	JPG	59.0KB	556x143		
	Name Stego Image	**Jenis Cover Data**	**Ukuran Cover Data**	**Resolusi Cover Data**		
	encrypted_encoded_Grandparents	PNG	674KB	556x143		

Figure 7 Byte-byte Image File Cover / Stego Image in Hexadecimal

The bitmap header file information lies in the first 14 bytes (0x0 to 0xE), then the bitmap header info info is located on the next 40 bytes (0xF to 0x53). The bitmap data pixel starts from the 55th byte (0x54) to the end of the bitmap file.At Figure above the yellow-colored bytes are pixel bytes of data before and after the message inserted. Visible change of pixel byte values by the data in accordance with the bits of the message is inserted. The byte values are arranged randomly so that the stego-data does not display visually or audio distortion.

4. CONCLUSIONS AND SUGGESTIONS

Based on the results of analysis and testing that has been done in the previous chapter, the conclusions that can be taken are as follows:

1. One of the security solutions that can be added is cryptografi to the secret message to be delivered. In this research applied security on steganography by adding ROT13 cryptography which make secret message then shifted 13 character. After encrypting the secret message is then inserted into the digital image by the method of Least Significant Bit (LSB) that is every bit of secret messages inserted in the last bit of digital images.
2. LSB meets Imperceptibility. The existence of a secret message cannot be perceived by the senses. For example, if a covertext is an image, then the insertion of a message makes the stegotext image difficult to distinguish by eye with its covertext image.
3. LSB meets the criteria of recovery. Messages can be extracted from stego-data and according to the message the sender means.

The following are suggestions that can be considered in developing this research. Suggestions that can be given by the author as a reference for the combination of MCO algorithm (multiple cover in subsequent research is as follows: In further research it is suggested that the media inserted secret messages can be audio or video files

DAFTAR PUSTAKA

[1] Nurhayati and S. S. Ahmad, "Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm," *2016 4th International Conference on Cyber and IT Service Management*, Bandung, 2016, pp. 1-6.

[2] S. Chauhan, Jyotsna, J. Kumar and A. Doegar, "Multiple layer text security using variable block size cryptography and image steganography," *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, Ghaziabad, 2017, pp. 1-7. S.

[3] M. Saritha, V. M. Khadabadi and M. Sushravya, "Image and text steganography with cryptography using MATLAB," *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, 2016, pp. 584-587.

[4] S. Sriram, B. Karthikeyan, V. Vaithiyanathan and M. M. A. Raj, "An approach of cryptography and steganography using rotor cipher for secure transmission," *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, 2015, pp. 1-4.

[5] M. P. Uddin, M. Saha, S. J. Ferdousi, M. I. Afjal and M. A. Marjan, "Developing an efficient solution to information hiding through text steganography along with cryptography," *2014 9th International Forum on Strategic Technology (IFOST)*, Cox's Bazar, 2014, pp. 14-17.

[6] Namita Tiwari, Dr.Madhu Shandilya," Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", International Journal of Computer Applications, Vol.6, No.2, Sep 2010.
[7] Munir, Rinaldi. 2006. Kriptografi. Bandung : Informatika.
[8] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2 Ariyus, Dony.. "Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi". Yogyakarta: Andi, 2008.
[9] B. J. Mohd, S. Abed, T. Al-Hayajneh, and S. Alouneh, "FPGA hardware of the LSB Steganography Method", IEEE International Conference on Computer, Information and Telecommunication Systems(CITS), pp. 1–4, 2012.