

# Text File Protection Using Least Significant Bit (LSB) Steganography and Rijndael Algorithm

Apri Siswanto<sup>1</sup>, Yudhi Arta<sup>1</sup>, Evizal Abdul Kadir<sup>1</sup>, Bimantara<sup>1</sup>

<sup>1</sup>Department of Informatics Engineering, Faculty of Engineering Universitas Islam Riau, Indonesia

{aprisiswanto@eng.uir.ac.id, yudhiarta@eng.uir.ac.id, evizal@eng.uir.ac.id, bimbinjabrikz@gmail.com}

**Abstract.** Nowadays, thousands of kilobytes personal data are transmitted every day through insecure communication media (such as the internet, computer networks, communication systems, etc.). This makes data vulnerable to information theft, especially for fraud, illegal trade and so on. So, there is a need for protecting the information in its storage and transmission. To improve data and information security, in this study, we propose a Least Significant Bit (LSB) steganography to insert message information in a 24-bit jpg image and Rijndael cryptography that is used to encrypt jpg images so that message information can be secured from unauthorized parties.

**Keywords:** Encryption, cryptography, LSB steganography, Rijndael, information hiding

## 1 Introduction

The rapid development of computer technology has triggered crimes that exploit the weaknesses of computer network transmission systems. One form of crime is hackers try to retrieve data and information through the transmission of computer networks or known as a man in the middle attack [1]. Transfer of essential data on companies, agencies, or the military is vulnerable to attack if it only relies on a standard security system[2]. Confidential information can be taken and used by irresponsible parties. So, this must be given special attention by the parties concerned. Some ways to overcome this problem is to secure the message using the information hiding technique. Information hiding is a field of science that studies how to hide messages so that they cannot be perceived (both visually and audial). There are two ways techniques used in information hiding i.e. cryptography and steganography [3].

Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, and authentication [4]. While Steganography is the science that studies, researches, and develops the art of hiding information. Steganography can be classified as one part of communication science [5]. In the digital information era, steganography is a technique and art of hiding

information and digital data behind other digital data, so that digital information is invisible.

Recently, some methods can carry out attacks on steganography by utilizing the weaknesses of steganography. These methods are Visual Attacks and Statistical Attacks [6]. Visual attacks explain the difference between noise and visual patterns, while statistical attacks to detect the steganography method used. Because the method of attack on steganography has been found, problems arise how to provide security for data so that data can be hidden. Besides, confidentiality can also be maintained from the parties who are not authorized to access it. Therefore, to increase data and information security, in this study, we implement message encryption (cryptography) while hiding data and information in image files.

This paper is organized as follows. Section two describes Rijndael and LSB steganography theory. Then, section three introduced literature review where different methods of hiding information are discussed. Next, Section four discusses the research method of this paper. After that, section five explained results and discussion. Finally, section six presents conclusions and references used at the end.

## 2 LSB Steganography and Rijndael Algorithm

LSB is a technique commonly used in encryption and decryption of confidential information. The way the LSB method works is to change the redundant bits of the cover image that have no significant effect on the bits of the secret message. Figure 1 showed the mechanism of the LSB method in 8-bit images by utilizing 4 bits LSB [7].

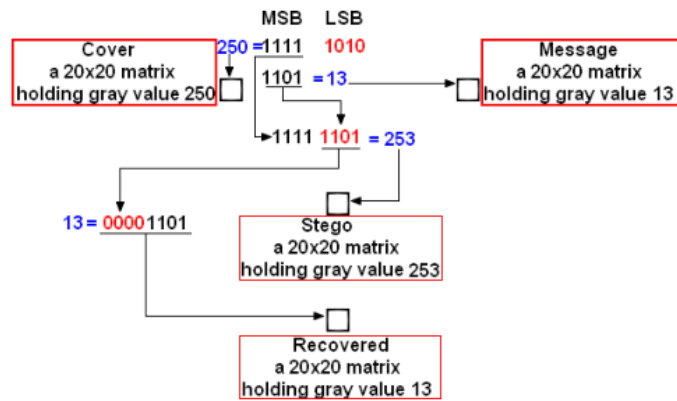


Figure 1: LSB Mechanism

Figure 1 showed the application of LSB using pixel-based image media with an 8-bit value (gray value). Each pixel consisting of 8 bits is divided into two parts, namely 4 bits MSB (most significant bits) and 4 bits LSB (least significant bits). The LSB part is changed to the value of the message to be inserted. After being sprinkled with a secret message, each pixel is rebuilt into a complete image resembling the original image media. The advantages of LSB is less suspicious in human eyes, easy to implement, and High perpetual transparency. On the other hand, the disadvantages of LSB include robustness and sensitivity to filtering, and scaling, rotation, the addition of noise in the image, and cropping can damage confidential messages [8].

The Rijndael algorithm used substitution, permutation, and a number of rounds. Each round used a different internal key. The key of each round is called around key. However, unlike DES operates bit-oriented, Rijndael operates in byte orientation. The goal is to minimize software and hardware resources. The Rijndael algorithm works on 128-bit blocks with 128-bit keys with the AddRoundKey process. AddRoundKey is to do XOR between the initial state (plaintext) and the cipher key [9]. This stage is also called initial round. The process carried out in each round is:

1. SubBytes: byte substitution using a substitution table (S-box).
2. ShiftRows: shifting array state lines in wrapping.
3. MixColumns: scrambles data in each state array column.
4. AddRoundKey: perform XOR between the current state of the round key.

The Rijndael algorithm has three parameters [10]:

1. plaintext: a 16-byte array, which contains input data.
2. ciphertext: an array of 16-byte size, which included the results of encryption.
3. key: an array of 16-byte size, which contains a ciphering key (also called a cipher key). With 16 bytes, both the data block and the 128-bit key can be stored in all three arrays ( $128 = 16 \times 8$ ).

### 3. Related Research

Data security and confidentiality are essential aspects needed in the process of exchanging data on the internet network. Two techniques can be used for data protection, namely cryptography and steganography. Several studies related to cryptography and steganography, for example, Syawal, et al., [11] proposed text message encryption using Vigenere cipher algorithm and LSB technique for inserting messages into images. The proposed encryption was programmed in MatLab 2014b. The object of research is to enter text into the image to produce hidden files and cannot be accessed by unauthorized parties.

Then, Purba et al., [12] has conducted a study Implementation of Text Message Steganography into Sound Files (.Wav) with Byte Distance Modification in the Least Significant Bit (Lsb) Algorithm. The purpose of this study is to hide files with the extension .txt and files ending in .Wav. Data bits are hidden or secured using LSB into the audio media. The result of the study found that the bit values are inserted into the audio media are still looks like normal so as not to arouse suspicion of the listener. Then if extracted, it will get back the whole bit values that have been inserted.

Therefore, the results of the research show that the resulting wav stego file has a good level of imperceptibility, fidelity, and recovery.

Utomo and Purnomo [13] has been proposed Image Steganography with the Least Significant Bit Method for Protection of Communication in Online Media. In this study, a message is inserted in the image file to be extracted again into a message. This method is done to secure the message and avoid unauthorized parties from utilizing the message.

The research conducted by Utomo and Purnomo, Purba et al., Syawal et al., and the research that the authors did together secure data by hiding the data into other data. The difference is in the object under study, the research method and the programming language used in developing the system. Like Purba, hide the .txt file into the file extension .Wav. Syawal used a different algorithm. And Utomo securing the message on the image file can then be extracted again into a message.

#### 4 Research Methodology

The LSB Steganography and Rijndael algorithm are implemented using the Visual basic net programming language. We used modified LSB steganography method as a medium that will hide text file information in the form of each bit data value into the image media bit values. Data bits that will be hidden or secured with LSB into the jpg image media. The proposed encryption scheme is like the figure 1.

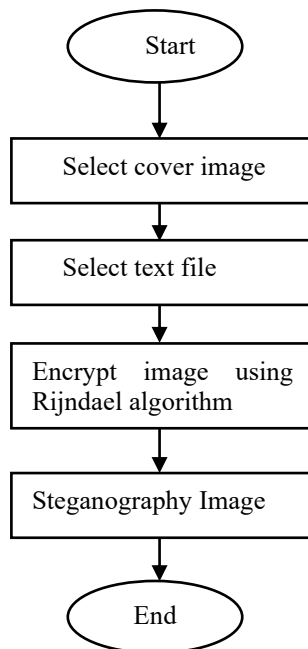
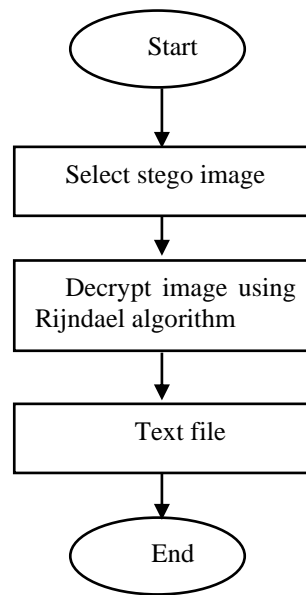


Fig. 1. Encryption process

In the encryption and decryption process, users must input object image files that will be steganography with text files that will be encrypted. Then the data is encrypted with the Rijndael algorithm. The Rijndael algorithm did the encryption process used substitution and permutation process. For the decryption process, the user enters the steganographic image file and then decomposes it with the Rijndael algorithm so that the ciphertext file returns to the original text file. See details in figure 2 the decryption process.



**Fig. 2.** Decryption process

## 5 Result and Discussion

This research output is an encryption scheme to secure text file. In simple application, the process steps is insert text files as a hidden message into a digital image. It is built using Visual Basic Net programming language, which has several supports for digital image programming. To accommodate the image when the process of hiding and reading the message, it used picture box control. The interface display of the application is like Figure 3.

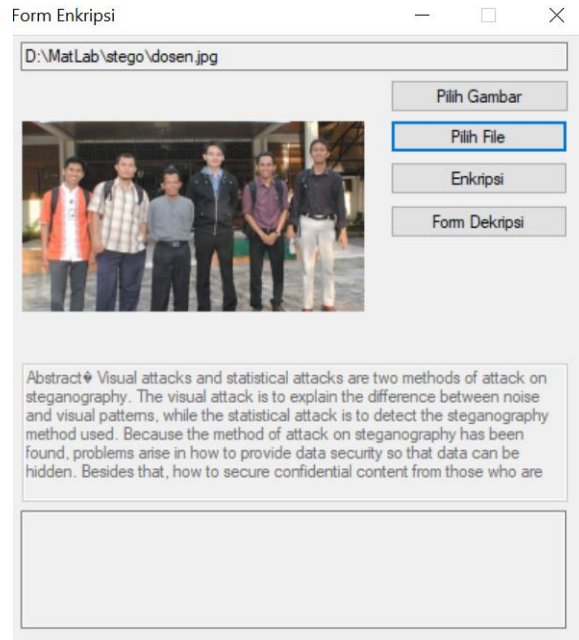


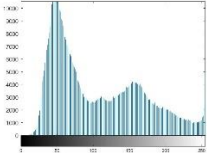
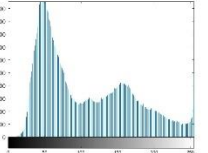


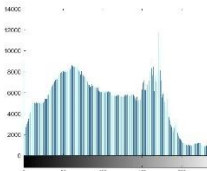
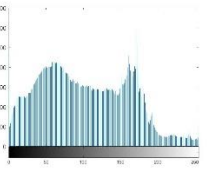


Fig. 3 Encryption decryption interface application

The first evaluation conducted was a histogram analysis. We have compared histogram analysis of the original image and stego image that has been inserted with the text file. The result is in table 1.

Table 1. Histogram analysis

| Original image (A)  | Stego image (B)   | Histogram A  | Histogram B   |
|---|---|--|---|
|  |  |  |  |
|  |  |  |  |

To determine image quality, the method of peak signal to noise ratio (PSNR) is used as a comparison of the quality of stego image with the original image (cover image). The term peak signal-to-noise ratio (PSNR) is a term in the field of engineering that states the ratio between the maximum possible signal strength of a digital signal and the noise power that affects the correctness of the signal. Because many signals have a wide dynamic range, PSNR is usually expressed on a logarithmic decibel scale [14]. The formula for calculating PSNR is as follows:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (1)$$

$$PSNR = 10 \cdot \log_{10} \left( \frac{MAX_1^2}{MSE} \right) \quad (2)$$

PSNR was defined through the signal-to-noise ratio (SNR). SNR is used to measure the level of signal quality. This value is calculated based on the comparison between the signal and the noise value. Signal quality is directly proportional to the SNR value. The higher the SNR value, the better the quality of the signal produced. Table 2 showed the results of calculation of values PSNR which is represented on a decibel scale (dB) [15].

Table 2. MSE, PSNE and MSE results

|             | <b>Image</b> | <b>MSE</b> | <b>PSNR</b> | <b>NSR</b> |
|-------------|--------------|------------|-------------|------------|
| Cover Image | Dosen.jpg    | 414.9138   | 22.0142     | 15.7063    |
| Stego Image | Dosen1.jpg   | 410.4317   | 21.9629     | 15.6550    |
| Cover Image | Kolam.jpg    | 408.2399   | 22.0304     | 15.3456    |
| Stego Image | Kolam1.jpg   | 404.2999   | 21.9541     | 15.2694    |

As the results of calculations in Table 1 show that the insertion of a text message with different sizes will produce different MSE and PSNR values. The larger the message file size, the higher the MSE value and the smaller the PSNR value, and vice versa the smaller the message file size, the smaller the MSE value and the higher the PSNR value. If the PSNR value is low, it can be said that image quality is getting worse, meaning that the image quality is physically bad. Whereas if the PSNR value is large, the image quality is still good, which means that the damage to the image is relatively small.

## 6 Conclusion

From the research that has been done, it can be concluded several things, namely steganography is a very efficient and powerful technique that allows to send text files safely and hidden. The LSB method that is applied to the message hiding process does not significantly affect the quality of the cover image.

## References

- [1] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and Network Security (Sie)*: McGraw-Hill Education, 2011.
- [2] A. Siswanto, A. Syukur, and I. Husna, "Perbandingan Metode Data Encryption Standard (DES) Dan Advanced Encryption Standard (AES) Pada Steganografi File Citra," in *Seminar Nasional Teknologi Informasi dan Komunikasi 2018*, 2018, pp. 190 - 197.
- [3] K. Challita and H. Farhat, "Combining steganography and cryptography: new directions," *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, vol. 1, pp. 199-208, 2011.
- [4] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*: CRC press, 1996.
- [5] R. Rahim, H. Nurdiyanto, R. Hidayat, A. S. Ahmar, D. Siregar, A. P. U. Siahaan, *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," in *Journal of Physics: Conference Series*, 2018, p. 012003.
- [6] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *International workshop on information hiding*, 1999, pp. 61-76.
- [7] M. Pelosi, N. Poudel, P. Lamichhane, D. Lam, G. Kessler, and J. MacMonagle, "Positive Identification of LSB Image Steganography Using Cover Image Comparisons," 2018.
- [8] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, pp. 727-752, 2010.
- [9] R. Munir, "Pengantar Kriptografi," *Penerbit Informatika Bandung*, 2010.
- [10] R. Munir, "Steganografi dan Watermarking," *Departemen Teknik Informatika, Institut Teknologi Bandung*. Diakses dari [http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Steganografi% 20dan% 20Watermark ing. pdf](http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Steganografi%20dan%20Watermarking.pdf), 2004.
- [11] M. F. Syawal, D. C. Fikriansyah, and N. A.-U. B. Luhur, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB," *Jurnal TICom*, vol. 4, 2016.
- [12] J. V. Purba, M. Situmorang, and D. Arisandi, "Implementasi steganografi pesan text ke dalam file sound (. wav) dengan modifikasi jarak byte pada algoritma least significant bit (LSB)," *Dunia Teknologi Informasi-Jurnal Online*, vol. 1, 2012.
- [13] P. Utomo and B. E. Purnama, "Pengembangan Jaringan Komputer Universitas Surakarta Berdasarkan Perbandingan Protokol Routing Information Protokol (RIP) Dan Protokol Open Shortest Path First (OSPF)," *IJNS-Indonesian Journal on Networking and Security*, vol. 1, 2012.
- [14] D. F. Alfatwa, "Watermarking Pada Citra Digital Menggunakan Discrete Wavelet Transform," *Bandung: Institut Teknologi Bandung*, 2005.
- [15] M. M. Amin, "Image Steganography dengan Metode Least Significant Bit (SLB)," *Jurnal Computer Science Research and Its Development (CSRID)*, vol. 6, 2014.