

# Smartcyber\_paper2

*by* Evizal Abdul Kadir

---

**Submission date:** 02-Jan-2021 02:57PM (UTC+0800)

**Submission ID:** 1482446511

**File name:** PROCEEDINGS\_SMART\_CYBER\_2020\_apri.pdf (414.37K)

**Word count:** 2469

**Character count:** 13173

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



Apri Siswanto, Yudhi Arta, Evizal Abdul Kadir, and Bimantara

**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. Siswanto (✉) · Y. Arta · E. A. Kadir · Bimantara

<sup>1</sup>Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau, Pekanbaru, Indonesia  
e-mail: [aprisiswanto@eng.uir.ac.id](mailto:aprisiswanto@eng.uir.ac.id)

Y. Arta

e-mail: [yudhiarta@eng.uir.ac.id](mailto:yudhiarta@eng.uir.ac.id)

E. A. Kadir

e-mail: [evizal@eng.uir.ac.id](mailto:evizal@eng.uir.ac.id)

Bimantara

e-mail: [bimbimjabrikz@gmail.com](mailto:bimbimjabrikz@gmail.com)

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

P. K. Pattnaik et al. (eds.), *Proceedings of International Conference on Smart Computing and Cyber Security*, Lecture Notes in Networks and Systems 149, [https://doi.org/10.1007/978-981-15-7990-5\\_20](https://doi.org/10.1007/978-981-15-7990-5_20)

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 aspects of information security 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 2 describes Rijndael and LSB steganography theory. Then, Sect. 3 introduced literature review where different methods of hiding information are discussed. Next, Sect. 4 discusses the research method of this paper. After that, Sect. 5 explained results and discussion. Finally, Sect. 6 presents conclusions and references used at the end.

## 2 LSB Steganography and Rijndael Algorithm

LSB is a technique commonly used to encrypt confidential information and to decrypt it. The way the LSB method works is to change the cover image's redundant bits which have no significant effect on the bits of the secret message. Figure 1 showed the LSB method mechanism in 8-bit images by using 4 bits of LSB [7].

Figure 1 showed LSB application using the 8-bit pixel-based image media (gray value). Each 8-bit pixel is divided into two parts, namely 4 MSB bits (most significant bits) and 4 LSB bits (lowest significant bits). The LSB part of the message to be inserted is changed to the value. After each pixel has been sprinkled with a secret message, it is reconstructed into a complete image that resembles the original media. In human eyes, the advantages of LSB are less suspicious, easy to enforce, and high eternal transparency. On the other hand, LSB's drawbacks include robustness and

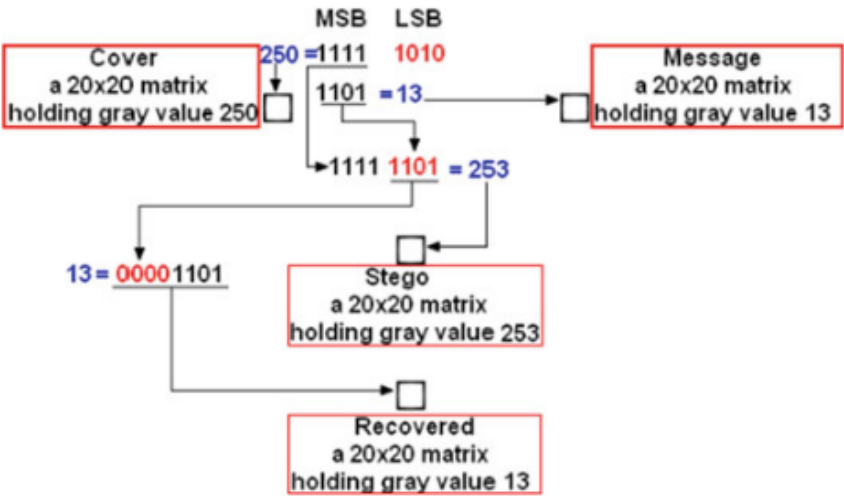


Fig. 1 LSB mechanism

sensitivity to filtering, and scaling, rotation, adding noise to 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 round 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 [13].

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 and 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 Purnama [13] have 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.

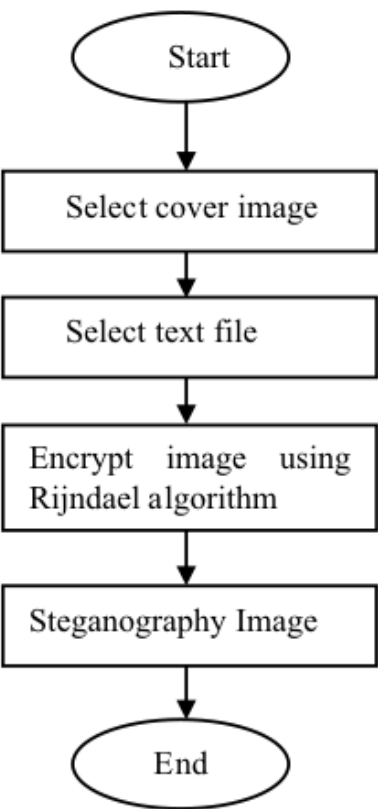
The research conducted by Utomo and Purnama, Purba et al., Syawal et al., and the research that the authors did together secure data by hiding the data into other data. The difference is in the object under study, the research method, and the programming language used in developing the system. Like Purba, 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

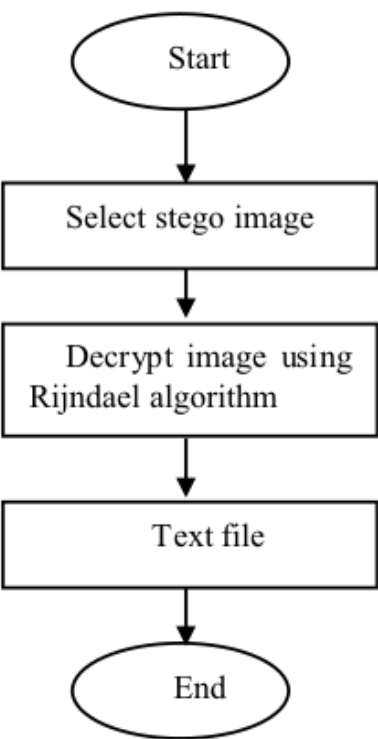
The LSB steganography and Rijndael algorithm are implemented using the Visual Basic Net programming language. We used modified LSB steganography method as a medium that will hide text file information in the form of each bit data value into the image media bit values. Data bits that will be hidden or secured with LSB into the jpg image media. The proposed encryption scheme is like Fig. 2.

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 using 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 Fig. 3 the decryption process.

**Fig. 2** Encryption process



**Fig. 3** Decryption process



### 5 Result and Discussion

This research output is an encryption scheme to secure text file. In simple application, the process steps are 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 Fig. 4.

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 `12.txt` file. The result is in Table 1.

The peak signal-to-noise ratio (PSNR) method is used to determine image quality as a comparison of the quality of the stego image with the original image (cover image). The term peak signal-to-noise ratio (PSNR) is a term in the engineering field that states the ratio between a digital signal's maximum possible signal strength and the noise power that affects the signal's correctness. Since many signals have a broad range of dynamics, PSNR is usually expressed on a logarithmic decibel scale [14].

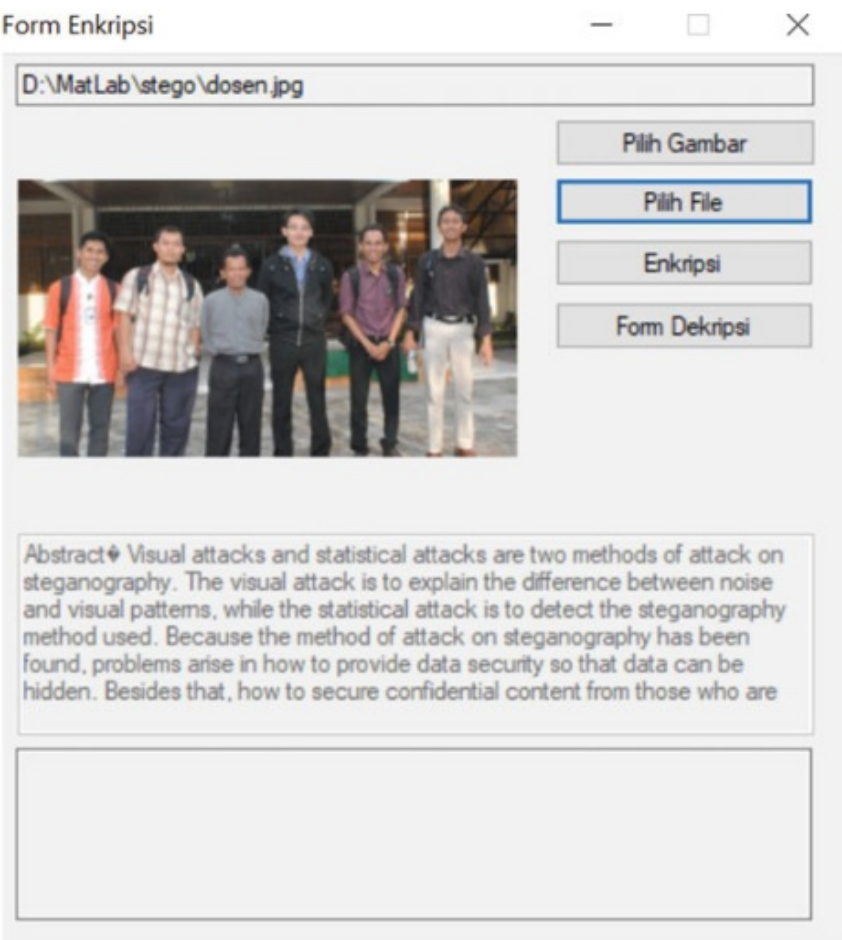







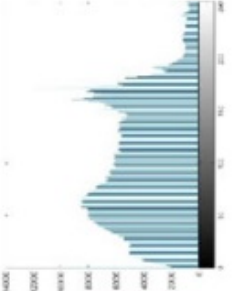


Fig. 4 Encryption/decryption interface application

Table 1 Histogram analysis

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



**Table 2** MSE, PSNE, and MSE results

Image		MSE	PSNR	NSR
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

The formula for calculating PSNR is as follows:

11

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

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

6  
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].

3  
As the calculation results in Table 2 show, inserting a text message with different sizes will yield different MSE and PSNR values. The greater the size of the message file, the higher the value of MSE and the smaller the value of PSNR, the smaller the size of the message file, the smaller the value of MSE and the higher the value of PSNR. If the PSNR value is low, it can be said that the image quality is getting worse, which means the quality of the image is physically poor. Whereas the image quality is still good if the PSR value is large, which means that the damage to the image is relatively small.

1

## 6 Conclusion

1  
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, D. Mukhopadhyay, *Cryptography and Network Security (Sie)* (McGraw-Hill Education, New York, 2011)
2. A. Siswanto, A. Syukur, 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, H. Farhat, Combining steganography and cryptography: new directions. *Int. J. New Comput. Archit. Appl. (IJNCAA)* **1**, 199–208 (2011)
4. A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, 1996)
5. R. Rahim, H. Nurdyanto, R. Hidayat, A.S. Ahmar, D. Siregar, A.P.U. Siahaan et al., Combination Base64 algorithm and EOF technique for steganography. *J. Phys. Conf. Ser.* **012003** (2018)
6. A. Westfeld, 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, J. MacMonagle, Positive Identification of LSB Image Steganography Using Cover Image Comparisons (2018)
8. A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: survey and analysis of current methods. *Sig. Proc.* **90**, 727–752 (2010)
9. R. Munir, Pengantar Kriptografi, in *Penerbit Informatika Bandung* (2010)
10. R. Munir, Steganografi dan Watermarking, in *Departemen Teknik Informatika, Institut Teknologi Bandung*. Diakses dari <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Steganografi%20dan%20Watermarking.pdf> (2004)
11. M.F. Syawal, D.C. Fikriansyah, N.A.-U.B. Luhur, Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB. *Jurnal TICOM* **4** (2016)
12. J.V. Purba, M. Situmorang, 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* **1** (2012)
13. P. Utomo, B.E. Purnama, Pengembangan Jaringan Komputer Universitas Surakarta Berdasarkan Perbandingan Protokol Routing Information Protokol (RIP) Dan Protokol Open Shortest Path First (OSPF). *IJNS-Indonesian J. Networking Secur.* **1** (2012)
14. D.F. Alfatwa, Watermarking Pada Citra Digital Menggunakan discrete wavelet transform, in *Bandung: Institut Teknologi Bandung* (2005)
15. M.M. Amin, Image steganography dengan metode least significant bit (SLB). *J. Comput. Sci. Res. Dev. (CSRID)* **6** (2014)

ORIGINALITY REPORT

19%	11%	10%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	e-journal.uajy.ac.id Internet Source	3%
2	Panji Rachmat Setiawan, Abdul Syukur, Novendra Kurniadi, Amrizal Amrizal. "Chapter 31 Android-Based Online Attendance Application", Springer Science and Business Media LLC, 2021 Publication	3%
3	Submitted to Universitas Siswa Bangsa Internasional Student Paper	2%
4	Submitted to Edith Cowan University Student Paper	2%
5	Nurhayati, Syukri Sayyid 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, 2016 Publication	2%
6	archive.org Internet Source	1%
7	eprints.dinus.ac.id Internet Source	1%
8	Okfalisa, Novi Yanti, Wahyu Aidil Dita Surya, Amany Akhyar, A Ambarwati Frica. "Implementation of Advanced Encryption	1%

Standard (AES) and QR Code Algorithm on Digital Legalization System", E3S Web of Conferences, 2018

Publication

9

Yudhi Arta, Evizal Abdul Kadir, Ari Hanggara, Des Suryani, Nesi Syafitri. "Chapter 15 Implementation of Motorcycle Monitoring Using Bluetooth with an Android-Based Microcontroller Using Arduino", Springer Science and Business Media LLC, 2021

1%

Publication

10

www.coursehero.com

Internet Source

1%

11

Submitted to SASTRA University

Student Paper

1%

12

Submitted to University of Bedfordshire

Student Paper

1%

13

journal.ugm.ac.id

Internet Source

1%