

Implementation of LSB (Least Significant Bit) Steganography on Image Files Using the 3DES (Triple Data Encryption Standard) Algorithm

Dodi Devrian Andrianto¹, M. Asyroful Nur Maulana Yusuf² and Makruf Alkarkhi³

^{1,2, n}Technical Information

Sumatran Institute of Technology (ITERA)

dodi.119140023@student.itera.ac.id¹, muhammad.119140026@student.itera.ac.id²,
makruf.119140075@student.itera.ac.id³

ARTICLE INFO

Keywords:

Cryptographic, Least Significant Bit, Triple Data Encryption Standard, Steganography

ABSTRACT

In this study, we propose the application of LSB (Least Significant Bit) steganography to image files with the 3DES (Triple Data Encryption Standard) algorithm, with the hope of helping digital information media users in sending and receiving data or information and secret messages safely. The research method we use is 3DES + LSB Implementation Using Image Citra and 3DES + MD5 Hash Innovation in .txt Files. The results and discussions described include, among others, Pseudocode, Cryptographic Testing, and Steganography Testing. Based on the results of program analysis and testing, it can be concluded that: The more messages that are inserted in the image, the more pixel differences in the stego image. The more colors in the image to which the message will be inserted, the more pixel differences in the stego image will be. The images that can be presented by stego objects are only images with .png and .jpeg extensions. The key used in the 3DES cryptographic algorithm consists of 24 letters. The key used in the 3DES + MD5 cryptographic algorithm can be varied. The combination of 3DES and LSB methods is able to maintain message security because it does not change the state or shape of the image. The combination of 3DES and MD5 methods only applies to .txt files.

1. INTRODUCTION

In the era of increasingly advanced technology as it is today, the use of digital information media to communicate and send and receive important data has become a necessity until later. Confidentiality and data security are very important in digital information media or current information systems, taking data or information to other parties can harm those who have data or information. (Hidayat Faizin, 2019) Confidential data or information is very valuable for the owner of the data or information, coupled with a very fast internet network and not guaranteed security. So it takes an effort to deal with this problem, one of these efforts is to apply cryptographic techniques. (Kumbara Pakereng, 2019)

Cryptography is a study that studies techniques or methods on how to process a confidential data or information, aiming to secure confidential data or information by carrying out encryption and decryption processes on data or information to be secured. (Febriani, 2019) Encryption is a process where data or information is converted into another form that is difficult to understand, meanwhile decryption is a process where data or information that has been converted into another form is returned to its original or original form. One of the data or information that is kept secret is the image, while the technique for securing the image is Steganography. (Kuncoro, 2019)

Steganography is a technique found in cryptographic studies that has uses as hiding information into a medium such as images, video, and sound. (Simbolon, 2021) An example of the application of steganographic techniques is that if there is an image that is inserted with information, the information will not be visible in the image that has been inserted, but if the image is extracted using special software steganography then the information that is inserted will be visible. (Bakir, 2018)

A method contained in image media steganography is called Least Significant Bit (LSB). The Least Significant Bit (LSB) method is a method used to insert information that goes through the process of replacing bits to 8, 16, and 24 in a binary image of an image file with a binary image of confidential information to be secured. (Nirmala, 2020)

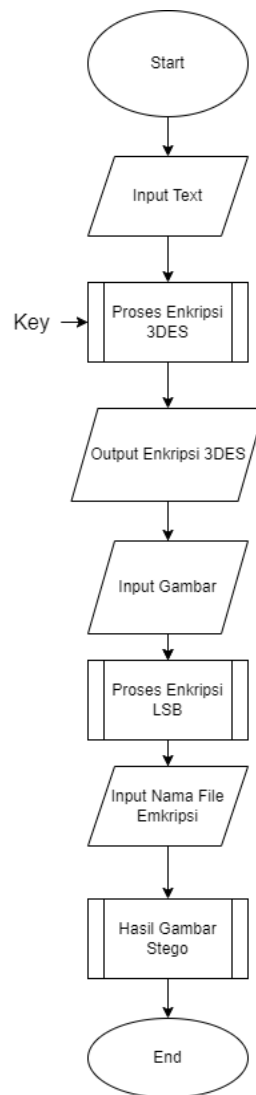
Triple Data Encryption Standard(3DES) is a development of the previous encryption system, namely the Data Encryption Standard (DES), the encryption system on 3DES has three layers and is certainly more secure than DES. At the time the DES algorithm was created, a key size of 56 bits was considered sufficient at that time. (Hariman, 2020) However, with the development of technology, computing attack capabilities have also increased, so 3DES was created by providing a simple method and increasing the DES key size to prevent computing attacks, by not using a new block cipher or block cipher. (Basim, 2020)

In this study we propose the implementation of LSB steganography (*Least Significant Bit*) on image files using the 3DES (Triple Data Encryption Standard) algorithm, with the hope of helping users of digital information media in sending and receiving data or information and secret messages safely.

2. RESEARCH METHODS

a. 3DES + LSB Implementation Using Image Image

The process of designing algorithms for steganography using the Least Significant Bit (LSB) method on image files using the Triple Data Encryption Standard (3DES) algorithm follows the path shown in the figure below.



The stages or flow in image processing in the image ... are as follows:

1. The user inputs the ciphertext which will be encrypted and inserted in the image,
2. The 3DES encryption process is carried out by adding a predefined key consisting of 24 letters.
3. The program will display the results of the 3DES encryption of the plaintext entered by the user.
4. The user inputs an image that will be used as a medium to insert a message.
5. LSB encryption process by inserting 3DES encryption results from the ciphertext.
6. The user will input the name of the stego file with the desired extension.
7. The program will perform and generate processes from the stego image that has been inserted text from the 3DES encryption result.

The image resulting from the insertion of a text message that has been encrypted 3DES above is called a stego image (Steganography). The next image shows a flowchart or flowchart on the return of text from the inserted stego image, resulting in the original message from the image.



Stages or flow in data processing on the stego image:

1. The user inputs the name of the stego image with the extension.
2. The extraction process on the stego image using the Least Significant Bit (LSB) method to see the message on the stego image.
3. The program displays a random text message on the stego image.
4. The random text message decryption process uses the Triple Data Encryption Standard (3DES) method.
5. The program displays plaintext results.

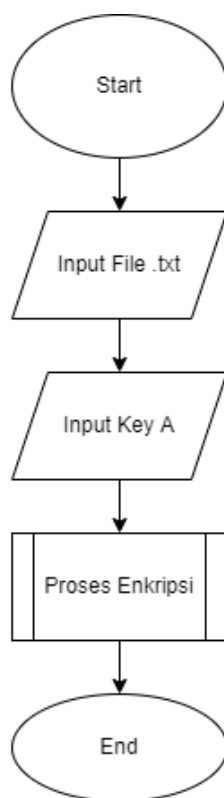
This program uses the pycryptodome module or package which functions to implement cryptography in python by using a library as shown below:

```
from base64 import b64encode, b64decode
from Crypto.Cipher import DES3
from Crypto.Util.Padding import pad, unpad
from PIL import Image
import sys
import numpy as np
```

1. from base64 import b64encode,b64decode serves to convert bytes of encryption or decryption of binary data or text into ASCII characters. The base64 encoding consists of 26 uppercase letters, 26 lowercase letters, 10 numbers, + and / for newlines.
2. from Crypto.Cipher import DES3 serves to protect data confidentiality by using the Triple Data Encryption Standard (3DES) method with encryption and decryption of a plaintext.
3. from Crypto.Util.Padding import pad,unpad to provide support for adding and removing standard padding from data.
4. from PIL import Image serves to import images in python programs.
5. import sys works for manipulation of various parts of the python runtime environment.
6. import numpy as np serves to perform algebraic processing in python.

b. 3DES Innovation + MD5 Hash on .txt Files

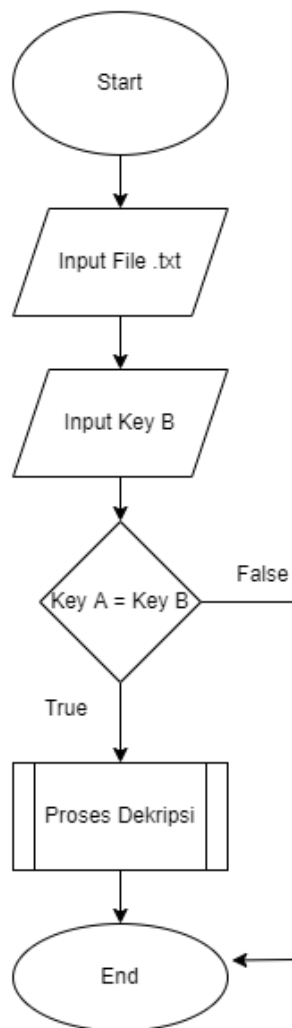
Furthermore, regarding the innovation of Triple Data Encryption Standard (3DES) cryptography by adding the MD5 Hash function to the .txt file, the following is a flowchart or flowchart of 3DES + MD5 Encryption in a .txt file:



Steps or flow in 3DES + MD5 Encryption in .txt files:

1. The user is asked to input the .txt file using the directory path.
2. The user inputs a key or keys.
3. The program performs the 3DES + MD5 encryption process.
4. In the .txt file the contents are changed to the results of the encryption process.

Furthermore, after the 3DES + MD5 encryption process is complete, then the following is a flowchart or flowchart on 3DES + MD5 Decryption in the .txt file:



The steps or flow in decrypting the .txt file are as follows:

1. The user is asked to input a .txt file with a directory path.
2. The user is asked to enter a key or keys.
3. After that, it goes through a branching process where, if key A = key B, the 3DES + MD5 decryption process will be carried out and if key A is not the same as key B, then the 3DES + MD5 decryption process will not go through.

After the 3DES + MD5 decryption process has been carried out, the .txt file will again contain the original text message.

This program uses the pycrypto, pycryptodome, and opencv-python modules, functions to apply cryptography and input .txt files in python. The following libraries are used for the 3DES + MD5 program:

```
fromCrypto.CipherimportDES3
fromCryptodome.CipherimportDES3
fromhashlibimportmd5
```

1. from Crypto.Cipher import DES3 serves to protect data confidentiality by using the Triple Data Encryption Standard (3DES) method with encryption and decryption of a plaintext in python.

2. from Cryptodome. Cipher import DES3 serves to protect data confidentiality by using the Triple Data Encryption Standard (3DES) method with encryption and decryption of a plaintext in python.
3. from hashlib import md5 serves to call the md5 hash function on python files as an innovation of the encryption and decryption program on 3DES programmed python.

3. RESULTS AND DISCUSSION

a. Pseudocode

In this program using the python programming language where there are two innovations carried out, the first innovation is implementing the 3DES + LSB cryptographic algorithm on image files and the second innovation implementing the 3DES + MD5 cryptographic algorithm on .txt files.

The first innovation regarding the implementation of cryptography and steganography on 3DES + LSB using the key = abcdefghijklmnopqrstuvwxyz, can be seen in the program code below:

```
key = b'abcdefghijklmnopqrstuvwxyz' #24 letter key
```

Encryption in the 3DES algorithm uses "ascii" and MODE_EAX encoding. As the encryption keyword in python, use encrypt like the program code below:

```
def encrypt(message):
    enc = DES3.new(key, DES3.MODE_EAX)
    nonce = enc.nonce
    ciphered_encode = enc.encrypt(message.encode('ascii'))
    return nonce, ciphered_encode
```

Decryption in the 3DES algorithm uses keywords in the python program, namely decrypt and decode as in the program code below:

```
def decrypt(nonce, ciphertext):
    dechipered = DES3.new(key, DES3.MODE_EAX, nonce=nonce)
    toplain = dechipered.decrypt(ciphertext)
    return toplain.decode('ascii')
```

The encryption process in steganography uses the LSB (Least Significant Bit) algorithm by paying attention to the RGB (Red, Green, Blue) pixels with n = 3 and RGBA (Red, Green, Blue, Alpha) with n = 4. as in the program code below this :

```
def Encode(src, message, dest):
    img = images.open(src, 'r')
    width, height = img.size
```

```

array = np.array(list(img.getdata()))

    if img.mode == 'RGB':
n = 3
    elif img.mode == 'RGBA':
n = 4

total_pixels = array.size // n

message += "$t3g0"
b_message = ''.join([format(order(i), "08b") for i in message])
req_pixels = len(b_message)

    if req_pixels > total_pixels:
        print("ERROR: Need larger file size")

    else:
index = 0
        for p in range(total_pixels):
            for q in range(0, 3):
                if index < req_pixels:
array[p][q] = int((son(array[p][q])[2:9] + b_message[index], 2))
                index += 1

array = array.reshape(height, width, n)
enc_img = Image.fromarray(array.astype('uint8'), img.mode)
enc_img.save(dest)

        print("Image Encoded Successfully")

```

The decryption process in steganography uses the LSB (Least Significant Bit) algorithm by paying attention to the RGB (Red, Green, Blue) pixels with $n = 3$ and RGBA (Red, Green, Blue, Alpha) with $n = 4$. as in the program code below this :

```

def Decode(src):

img = images.open(src, 'r')

array = np.array(list(img.getdata()))

```



```

    if img.mode == 'RGB':
n = 3

    elif img.mode == 'RGBA':
n = 4

total_pixels = array.size // n

hidden_bits = ""

    for p in range(total_pixels):
        for q in range(0, 3):
            hidden_bits += (son(array[p][q][2:][-1]))

hidden_bits = [hidden_bits[i:i+8] for i in range(0,
len(hidden_bits), 8)]

message = ""

    for i in range(len(hidden_bits)):

        if message[-5:] == "$t3g0":
            break

        else:
            message += chr(int(hidden_bits[i], 2))

        if "$t3g0" in message:

            print("Hidden Messages:", message[:-5])

        else:

            print(enc)

```

The second innovation regarding the implementation of cryptography with the 3DES + MD5 algorithm, which uses the DES3 and MD5 keywords in python programming as the program code below:

```
key_hash = md5(key.encode('ascii')).digest()
```

```
tDES_key = DES3.adjust_key_parity(key_hash)

cipher = DES3.new(tDES_key, DES3.MODE_EAX, nonce=b'0')
```

b. Cryptographic Testing

In this program, the researcher tested the data by comparing between 3DES without using the MD5 Hash function and the 3DES program using the MD5 Hash function. The comparison is carried out with the scenario of entering 3 different messages and using the same key because the key for the 3DES process without the MD5 function cannot be entered by the user.

By doing this comparison, the researcher got the data from the test. These data are:

Text Message	Character Length	Key	3DES Results	Character Length	Results 3DES + MD5	Character Length
informatics engineering study program	24	abcdefghijklmnpqrstuvw	2OABMdg mJM0w/Vf vkFbdbl2 3pvmjQ8	32	j? ? ? ? ? ? } ? ? - ?] ? ? hW ? ~ ? G _	24
cryptograph y course	22	abcdefghijklmnpqrstuvw	FPcVeGgn eWlBhaNB P3ZSESU7 iYY4iQ==	32	w ? ? ? ? ? q ? - ?] ? ? hB ? ~ ? G	22
good coding	14	abcdefghijklmnpqrstuvw	Xu+Sz0sX h+znLwIk yhQ=	20	t ? ? ? ? ? 8 ? ? ? 2 ? R	14

From the table above, it is known that the more characters of a text message, the more 3DES encryption results are generated. The results of 3DES encryption using the MD5 Hash function and 3DES without using the MD5 Hash function have differences in the shape and number of characters. When using the MD5 Hash function, the resulting character length remains the same as the initial message takes character length. However, when without using the MD5 Hash function, the encrypted character length is different from the initial message character length.

c. Steganography Testing

In this program, researchers tested the data by analyzing three scenarios. The first scenario, the researcher makes a comparison using the same object and different messages. Then the second scenario performs a comparison using different objects and the same message. The latter performs comparisons using different objects with different messages as well.

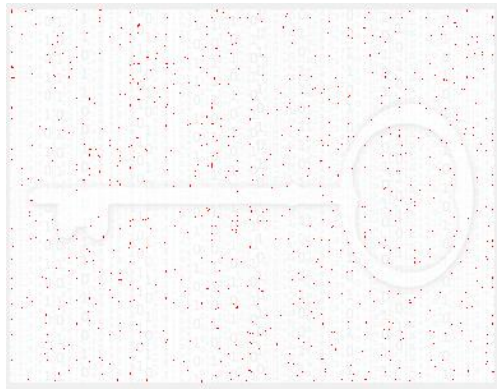
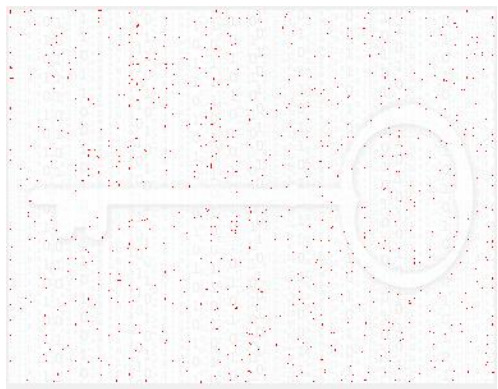
From the three test results that have been carried out, there is a change in the pixels between the image before the word is inserted and after it is inserted. However, at a glance, the two images do not look the difference. To find out how many different pixels are, the researcher uses the help of a website to compare images. The website is [isaimagekit.com](https://www.isaimagekit.com).

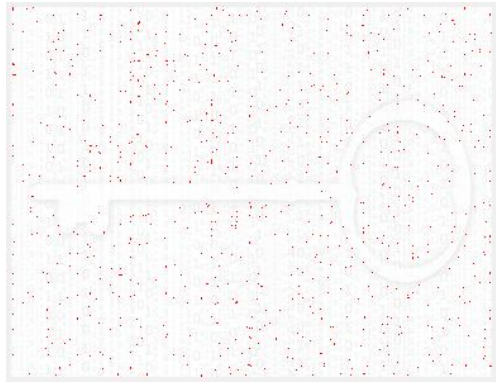

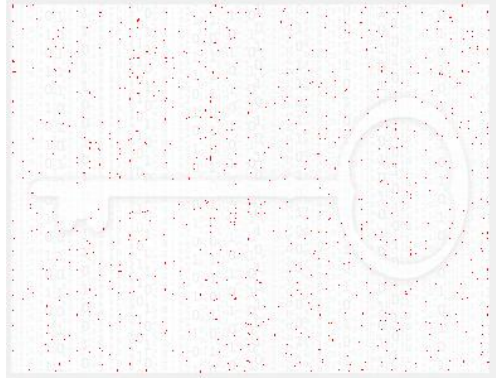

By doing this comparison, the researcher got the data from the test. These data are:

Scenario	Pixel Difference		Difference pixel difference	Message	
	Process 1	Process 2		Order 1	Order 2

Same Object Different Message	845	846	1	cryptography course	informatics engineering study program
Different Object Same Message	844	95	749	itera campus	itera campus
Different Objects Different Messages	844	97	747	healthy coding	good coding

The results of the data, evidenced by the placement of different pixels, for more details see the image below:

Parameter	Place the Difference
Same Object Message Different Process 1	
Same Object Message Different Process 2	

Object Different Message Same Process 1	
Objects Different Message Same Process 2	
Different Object Message Different Process 1	
Different Object Message Different Process 2	

4. CONCLUSIONS AND RECOMMENDATIONS

Based on the results of program analysis and testing, it can be concluded that:

1. The more messages that are inserted in the image, the more pixel differences in the stego image.
2. The more colors in the image to which the message will be inserted, the more pixel differences in the stego image will be.
3. The images that can be presented by stego objects are only images with .png and .jpeg extensions.
4. The key used in the 3DES cryptographic algorithm consists of 24 letters.
5. The key used in the 3DES + MD5 cryptographic algorithm can be varied.

6. The combination of 3DES and LSB methods is able to maintain message security because it does not change the state or shape of the image.
7. The combination of 3DES and MD5 methods only applies to .txt files.

The recommendations given by the researcher to the next researcher regarding the 3DES (Triple Data Encryption Standard) cryptographic algorithm are:

- a. 3DES and LSB innovations can serve stego objects with extensions other than .png and .jpeg
- b. The combination of 3DES and MD5 methods can encrypt plaintext in ascii (b64encode) form.
- c. The keys to the 3DES cryptographic algorithm are more varied.
- d. Perform tests with more parameters.

References

- Hidayat, A., & Faizin, A. (2019). Comparison of Cryptography Using Data Encryption Standard Algorithm (DES) And Rivest Shamir Adleman Algorithm (RSA) For Data Security. *JASIEK (Journal of Applications of Science, Information, Electronics and Computers)*, 1(2). doi:10.26905/jasiek.v1i2.3451
- Kumbara, PB, & Pakereng, MA (2019). Design of Block Cipher Cryptography Techniques based on the traditional Rangku Pestle Game Pattern. *Journal of Informatics and Information Systems Engineering*, 5(2). doi:10.28932/jutisi.v5i2.11714
- Nursobah, N., Lailiyah, S., & Kurnia, A. (2020). Implementation of Text Message Steganography Into Audio Files (.MP3) with advanced encryption standard and least significant bit ALGORITMA. *IT JOURNAL*, 10(2), 122-139. doi:10.37639/jti.v10i2.152
- Nirmala, E. (2020). The application of image file steganography uses the least significant bit (LSB) method and the android-based advanced encryption standard (AES) cryptographic algorithm. *Journal of Informatics Pamulang University*, 5(1), 36. doi:10.32493/informatika.v5i1.4646
- Simbolon, BJ (2021). Message embedding steganography in image files by using the LSB (least significant bit) method. *National Journal of Computing and Information Technology (JNKTI)*, 4(1), 1-6. doi:10.32672/jnkti.v4i1.2656
- Permana, AA (2021). Message Security using Steganography Technique with Least Significant Bit (LSB) Algorithm. *Journal of Algorithms, Logic and Computing*, 3(2). doi:10.30813/j-alu.v3i2.2477
- Putra, ZN, & Prihanto, A. (2020). Application of Steganography Using the method of least significant bit (LSB) and pixel value differencing (PVD) on color images. *Journal of Informatics and Computer Science (JINACS)*, 1(03), 165-173. doi:10.26740/jinacs.v1n03.p165-173
- Marudin, M., & Windarto, W. (2021). Implementation of least significant bit (LSB) Steganography on desktop-based applications at BSA land property developer. *SKANIKA*, 4(2), 57-62. doi:10.36080/skanika.v4i2.2434

- Anshori, Y., Dodu, AE, & Purwaningsih, M. (2019). Application of Steganography In digital image media using the least significant bit (LSB) method. SATIN - Information Science And Technology, 5(1), 1-10. doi:10.33372/stn.v5i1.435
- Kuncoro, TR, & Aditama, R. (2019). Analysis of the combination of the RSA cryptographic algorithm and the least significant bit (LSB) Steganography algorithm in securing digital messages. STATMAT : JOURNAL OF STATISTICS AND MATHEMATICS, 1(2). doi:10.32493/sm.v1i2.2947
- Basim, Z., & Painem. (2020). Implementation of Cryptography Algorithm RC4 and 3DES and Steganography with EOF Algorithm for Desktop-Based Data Security at SMK As-Su'udiyah, 3.
- Hariman, AM, & Puspasari, R. (2020). Comparison of 3DES Method with AES for Securing Android Based Image Files, 1.
- Bakir, & Hozairi. (2018). Implementation of the Least Significant Bit (LSB) Method with Caesar Cipher Encryption in Steganography Using Image Processing, 3.
- Gunawan, HA, Arifin, Z., & Astuti, IF (2014). Web Login Security Using 3DES Method Based on Quick Response Code Technology, 9.
- Febriani, SI, Juanita, S., & Hardjanto, M. (2019). Implementation of Text Cryptography in SMS Using Multiple Encryption Algorithm with RSA and 3DES Methods, 15.