DINAMIKA REKAYASA
http://dinarek.unsoed.ac.id

**Vol. 12 No. 2 (2018) Hal. 104-111**
**p-ISSN** 1858-3075 **| e-ISSN 2527-6131**

# MODIFIKASI ENKRIPSI GAMBAR MENGGUNAKAN 64-BIT KUNCI PADA ALGORITMA DATA ENCRYPTION STANDARD (DES)

## MODIFICATION OF IMAGE ENCRYPTION USING 64-BIT KEY ON DATA ENCRYPTION STANDARD (DES) ALGORITHM

**Ibnu Utomo Wahyu Mulyono*, Wellia Shinta Sari, De Rosal Ignatius Moses Setiadi, Christy Atika Sari**

*Email: ibnu.utomo@dsn.dinus.ac.id

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Semarang, Indonesia

***Abstrak***— Proteksi data menggunakan teknik kriptiografi telah dilakukan sejak abad ke 14. Algoritma kriptografi sampai saat ini masih dapat digunakan dan mempunyai tingkat keamanan yang baik salah satunya yaitu *Data Encryption Standard* (DES). DES melakukan enkripsi dengan kunci simteris dengan panjang 64 bit kunci yang didapat dari kunci eksternal. Beberapa penelitian sebelumnya telah menggunakan DES pada media teks, dalam makalah ini DES telah digunakan pada media gambar. Gambar yang digunakan berukuran 512x512 piksel, dengan pesan berupa file .txt dengan panjang bervariasi antara 8 *byte* sampai dengan 1024 *byte*. Penggunaan file pesan yang bervariasi digunakan untuk mengetahui performa DES, baik dari segi waktu enkripsi dan dekripsi maupun hasil proses dekripsi. Hasil eksperimen menggunakan sejumlah pesan menghasilkan nilai *Peak Signal to Noise Ratio* (PSNR) tertinggi 86.7532 dB, dan waktu enkripsi pesan dengan ukuran kurang dari 64 bit tidak lebih dari 1 detik, sedangkan waktu dekripsi lebih cepat dibanding waktu enkripsi. Sedangkan nilai *Structural Similarity Index Mesurement* (SSIM) yang didapat yaitu 1.

***Kata kunci*** — DES, citra, enkripsi, PSNR.

***Abstract***— Data protection using cryptographic techniques has been done since the 14th century. Cryptography algorithm until now still can be used and have a good level of security one of which is Data Encryption Standard (DES). DES encrypts with a simteris key with a key length of 64 bits obtained from an external key. Several previous studies have used DES in text media, in this paper DES will be used on the image media. The image used is 512x512 pixels in size, with messages of .txt files with lengths varying between 8 bytes to 1024 bytes. The use of various message files is used to determine the performance of DES, both in terms of time of encryption and decryption as well as the results of the decryption process. The experimental results using a number of messages resulted in the highest Peak Signal to Noise Ratio (PSNR) value of 86.7532 dB, and a message encryption time of less than 64 bits in not more than 1 second, while decryption time was faster than the encryption time. Whereas, value of Structural Similarity Index Mesurement (SSIM) yielded 1.

***Keywords*** — DES, image, encryption, PSNR.

## I. PENDAHULUAN

Perkembangan layanan pada media sosial menyebabkan peningkatan pertukaran data, terutama citra digital. Mengirim gambar dalam bentuk polos dapat meningkatkan risiko disalahgunakan atau dicuri. Oleh karena itu, keamanan diperlukan dalam proses pertukaran gambar. Teknik keamanan dapat dilakukan dengan menerapkan teknik kriptografi [1] Kriptografi berasal dari bahasa Yunani *'Kryptos'* yang berarti tersembunyi atau rahasia dan *'Graphein'* berarti menulis [2]. Kriptografi adalah ilmu yang digunakan untuk mengamankan informasi yang dikomunikasikan dari pihak ketiga.

Sebagai metode yang diterapkan dalam proses pengamanan informasi, kriptografi dapat digunakan untuk mengamankan data penting. Data akan dikodekan menjadi simbol tertentu menggunakan kunci tertentu, yang akan menghasilkan karakter acak tanpa arti; Oleh karena itu, orang tertentu (yang mempunyai kunci) bisa mengetahui datanya.

Pada kriptografi ada pesan asli yang disebut *plaintext*, dan pesan terenkripsi disebut *ciphertext* [3]. Proses mengubah plaintext menjadi ciphertext disebut *enciphering* atau *encryption*. Proses mengembalikan *ciphertext* ke *plaintext* disebut menguraikan atau dekripsi. Dalam proses *enciphering* dan *deciphering* diperlukan *auxiliary variables* sebagai *key*. Menurut [4], salah satu metode kriptografi yang terkenal, dan sulit untuk dipecahkan dalam proses dekripsi data adalah *Data Encryption Standard* (DES). Menurut Kusuma, pada penelitiannya menyatakan bahwa DES mampu melakukan enkripsi sempurna pada media gambar [5]. Berdasarkan keunggulan yang dimiliki DES maka dalam makalah ini kami menyajikan hasil eksperimen enkripsi dekripsi dalam gambar *grayscale* dengan pesan berupa teks .txt.

## II. TINJAUAN PUSTAKA

### A. Penelitian Terkait

Beberapa penelitian terkait dengan algoritma DES pada teknik kriptografi telah dilakukan oleh Ardiansyah pada tahun 2018, dimana DES yang diimplementasikan dioperasikan sebanyak tiga kali untuk memdapatkan kemaman ganda pada saat melakukan proses *embedding* menggunakan algoritma *Arnold Transformation* atau dikenal dengan nam *Arnold Cat Map* (ACM). Hasil akhir menunjukkan bahwa DES tepat digunakan untuk proteksi data gambar yang dikombinasi dengan teknik steganografi [6].

Menurut Zaman [7], DES dalam implementasiya dengan bilangan acak *Pseudo Random Number Generator* (PRNG) GF 7 membuktikan bahwa panjang kunci dapat diterapkan antara 8 sampai 177 byte dan menghasilkan algoritma yang lebih tahan terhadap serangan. Hal ini terkait dengan bilangan polynomial yang digunakan untuk mengacak kunci. Penelitian yang dilakukan oleh Joseph [8], melakukan komparasi terhadap kunci simetris dan kunci asimetris. Dalam ekperimen tersebut dilakukan komparasi antara DES, 3DES, *Advance Encryption Standard* (AES), *Rivest Shamir Adleman* (RSA) dan *Message Digest* (MD5). Dalam penelitian ini ditemukan bahwa DES cocok digunakan pada bit 64, dengan konsumsi *energy* yang rendah sehingga cepat dalam pengoperasian dengan bilangan *festial*.

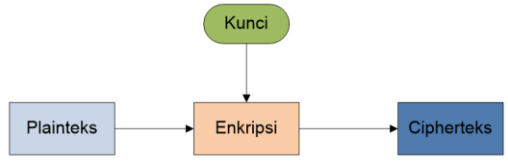
Penelitian lainnya menggunakan DES dilakukan oleh Prasetiyo [9] dengan mengkombinasikan operasi *bit matching* dalam teknik steganografi. Dengan objek berupa gambar berwarna dan pesan berupa teks, didapatkan hasil enkripsi tercepat yaitu 7,576 detik dan dekripsi tercepat yaitu 7,900 detik. Evaluasi lain dilakukan dengan perhitungan *Peak Signal to Noise Ratio* (PSNR) dalam serangan *salt and peper* dan *gaussian noise*.

### B. Kriptografi

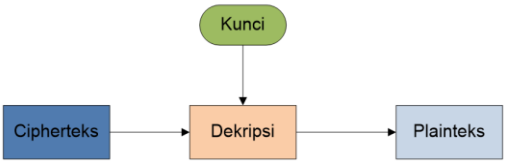
Kriptografi merupakan teknik kamuflase data dengan model perhitungan substitusi, permutasi dan transposisi. Teknik ini muncul 3000 tahun yang lalu [2]. Hingga saat ini kriptografi berkembang, dari kriptografi klasik menjadi kriptografi modern dengan berbagi algoritma. Dalam kriptografi klasik, tidak dikenal adanya kriptografi kunci simteris maupun asimetris. Hal ini berkebalikan dengan jenis kriptografi modern. Kriptografi klasik lebih menekankan pada pergeseran dan penggunaan operasi modulo kemudian menerapkan proses subtitusi pada 3 jenis cipher yaitu *monoalphabeth cipher*, *polyalphabeth cipher* [10], *polygram cipher*, dan *homofonik cipher*.

Cipher substitusi kemudian berkembang menjadi cipher transposisi. Bentuk cipher transposisi antara lain transposisi kolom, transposisi ro.iute, transposisi ganda, transposisi *myzkowsky*, transposisi *rail fence* [11]. Kemunculan cipher transposisi menyebabkan munculnya teknik super enkripsi. Teknik super enkripsi yaitu kombinasi dari substitusi cipher dan transposisi cipher, misalnya kombinasi *playfair* cipher dan transposisi kolom.

Dalam kriptografi terdapat 2 proses yaitu enkripsi dan dekripsi seperti tampak pada Gambar-1.




(a) Proses Enkripsi




(b) Proses Dekripsi

**Gambar-1**. Proses Enkripsi dan Dekripsi [12]

Pada Gambar-1 dapat dilihat bahwa proses kriptografi berjalan pada 2 buah proses yaitu enkripsi dan dekripsi. Proses enkripsi bertujuan merubah bentuk plainteks menjadi cipherteks, dimana plainteks adalah data awal dan cipherteks adalah data yangsudah tersandikan denga bantuan kunci. Proses dekripsi bertujuan untuk melakukan ekstraksi pada cipherteks dengan bantuan kunci. Kunci yang digunakan dalam enkripsi maupun dekripsi boleh sama atau berbeda. Hal ini disebut dengan kriptografi kunci simteris dan asimteris.

Menurut Cheddad dalam penelitiannya menyebutkan bahwa teknik kriptografi sangat berbeda dengan teknik kamuflase data lain seperti watermarking [13] dan steganografi [14]. Kriptografi berbeda dengan steganografi yang bertujuan untuk komunikasi rahasia dan konsentrasi penyembunyian datanya digunakan sebagai peningkatan kapasitas pesan yang tersembunyi. Hal ini lain dengan kriptografi yang bertujuan untuk proteksi data dimana media yang telah diproteksi dapat dikenali oleh mata manusia, namun data tersebut aman karena tersandikan.

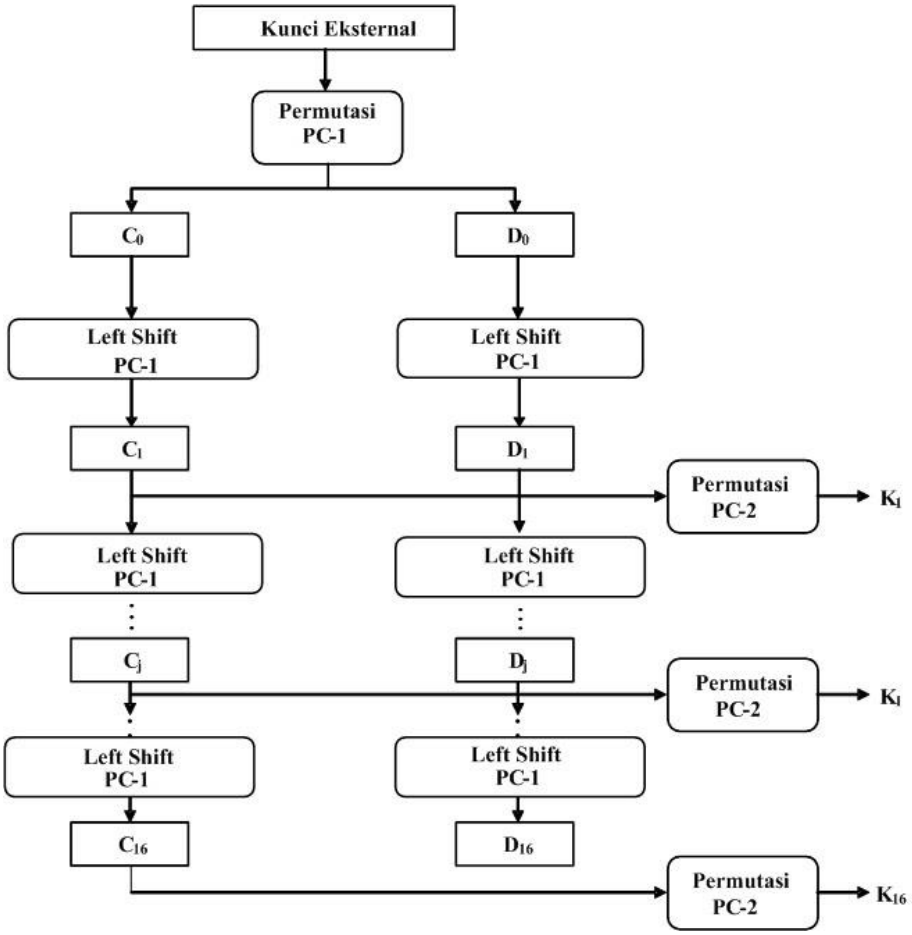
### C. Data Encryption Standard (DES)

*Data Encryption Standard* (DES) merupakan dalah satu algoritma kriptografi sinteris yang muncul pada tahun 1972. DES juga tergolong sebagai blok cipher dengan ukuran 64 bit.

DES mengubah 64 bit plainteks menjadi 64 bit cipherteks dengan bantuan kunci internal sebanyak 56 bit dan juga upa kunci. Kunci internal tersebut berasal dari kunci eksternal dengan panjang 64 bit. Proses perputaran dalam enkripsi DES dilakukan sebanyak 16 kali, hal ini dikarenakan jika putaran kurang dari 16 maka cipherteks dapat dideteksi oleh *known plaintext attack.*

## III. METODE PENELITIAN

Dalam penelitian ini, telah diterapkan skema enkripsi maupun dekripsi menggunakan algoritma *Data Encryption Standard* (DES) seperti pada Gambar-2.




**Gambar-2.** Tahapan Algoritma DES

Berdasarkan Gambar-2, maka tahapan operasi DES dapat direpresentasikan sesuai point berikut:

1. Ubah plainteks menjadi bilangan biner kemudian ubah 64 bit plainteks menggunakan tabel IP-Permutation pada Gambar-3.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

**Gambar-3**. Matriks IP-Permutation

2. Bagi nilai IP sebanyak 64 bit tadi menjadi L0 dan R0, masing-masing sepanjang 32 bit.
3. Lakukan pembangkitan kunci eksternal, dimana kunci juga diubah dalam bentuk biner terlebih dahulu. Kelompokkan bit kunci dengan ukuran masing-masing 8 bit.
4. Gantikan bit kunci tadi dengan tabel PC-1. Kunci awal 64 bit akan menjadi 56 bit saja.
5. Bagi kunci hasil PC-1 menjadi 2 bagian sama panjang, masing-masing 28 bit dengan nama C0 dan D0.
6. Buat 6 blok dengan nama Cn dan Dn yang berasal dari Cn-1 dan Dn-1. Pada setiap blok yang terbentuk, geser ke kiri sebanyak jumlah pergeseran.
7. Perhatikan jumlah pergeseran bit sesuai putaran dimana putaran ke 1, 2, 9 dan 16 hanya digeser sebanyak 1 bit sedangkan putaran lainnya digeser sebanyak 2 bit.
8. Lakukan putaran sampai 16 kali, sehingga didapatkan C16 dan D16.
9. Hasil geseran tadi kemudian dioperasikan dengan tabel PC-2, sehingga akan didapatkan kunci sebanyak 16 buah yaitu K1 sampai K16 pada Gambar-4.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 17 | 11 | 24 | 1 | 5 | 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

**Gambar-4**.Matriks PC-2

10. Lakukan proses enchipering dengan jairngan feistel, dari 32 bit menjadi 48 bit kembali. Proses substitusi bit dengan *E-Bit Selection Table* pada Gambar-5.

| | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

**Gambar-5.** Matriks E-Bit Selection

11. Lakukan perhoitngn XOR hasil *E(Rn-1)* dengan Key Kn.
12. Gunakan setiap 6 bit hasil dari $K_1 \oplus E(R_0)$ untuk menjadi alamat tabel yang dinamakan *S-Box*. Setiap kelompok 6 bit akan memberikan alamat pada masing-masing *S-box* yang berbeda.
13. Hitung nilai S1(B1) sampai S8(B8).
14. Lakukan proses permutasi pada hasil S-Box mengguankan tabel P berikut sehingga didapat kan nilai L0, R0, dan K1 pada Gambar-6.

| | | | |
|---|---|---|---|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

**Gambar-6**. Matriks Nilai L0,R0, dan K1

15. Lakukan 16 kali putaran untuk menghitung L1=R0, dan menghitung $R_2 = L_1 + f(R_1 , K_2 )$.
16. Setelah mendapatkan L16 dan R16 maka lakukan proses *reverse* dan lakukan proses permutasi dengan tabel $IP^{-1}$ pada Gambar-7.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

**Gambar-7**. Matriks Invers Inisial Permutasi $IP^{-1}$

17. Didapatkan cipherteks dalam bentuk heksadesimal.

Dalam eksperimen ini, tahapan DES diatas telah dilakukan pada *host* berupa gambar 512x512 piksel, *grayscale*, dan berformat .bmp. Pesan berupa teks dengan panjang teks bervariasi yaitu 8, 16, 32, 64, 128, 256, 512, sampai 1024 byte. Untuk detail *host* dan pesan yang digunakan dapat dilihat pada Gambar-8 dan Tabel-1.

**Gambar-8.** Cover Berupa Citra Ukuran 512x512 piksel

## IV. HASIL DAN PEMBAHASAN

**Tabel-1.** File Pesan dalam Format .txt

| Ukuran File (dalam Byte) | Isi File |
|---|---|
| 8 | del8apan |
| 16 | 16 enam belas 16 |
| 32 | De Rosal, Ignatius Moses Setiadi |
| 64 | Image Steganography Technique using LSB and One Time Pads Cipher |
| 128 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM |
| 256 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM |
| 512 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM |
| 1024 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM |

Setelah melakukan proses enkripsi, citra cover kemudian dibandingkan dengan citra hasil enkripsi seperti pada Tabel-2. Hal ini bertujuan untuk mengetahui pemenuhan proses kriptografi pada aspek *imperceptibility* atau ketidaknampakan oleh mata manusia. Dalam makalah ini, imperceptibility diukur dengan *Peak Signal to Noise Ratio* (PSNR). Nilai PSNR didapatkan dengan menghitung nilai MSE terlebih dahulu sesuai rumus (1) dan rumus (2).

Alat evaluasi lainnya yang digunakan pada penelitian ini yaitu *Standard Similarity Image Measurement (SSIM)*. Nilai SSIM tertinggi yaitu 1, artinya citra dalam keadaan tidak rusak dan sama seperti citra asli sebelum mengalami proses enkripsi.

Sedangkan menurut Hore [15], nilai PSNR lebih dari 40 dB menyatakan bahwa kualitas citra dalam keadaan baik dan dapat diterima oleh penglihatan manusia.

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{x} \sum_{y=1}^{y} \sum_{z=1}^{z} \|C_i(x,y,z) - S_i(x,y,z)\|^2 \quad (1)$$

$$PSNR = 10\, log_{10} \frac{2^8 - 1}{MSE} \quad (2)$$

dimana

MxN = ukuran citra asli
Ci = citra asli
Si = citra hasil enkripsi
x,y,z = layer citra

$$SSIM(A,B) = \frac{(2\mu_A\mu_B + c_1)(2\sigma_{AB} + c_2)}{(\mu_A^2+\mu_B^2+c_1)(\sigma_A^2 + \sigma_B^2 + c_2)} \quad (3)$$

dimana,

$\mu_A, \mu_B$ = *mean* dari citra A dan B

$\sigma_{AB}$ = covariance citra A terhadap B

$\sigma_A^2$ = varian dari citra A

$\sigma_B^2$ = varian dari citra B

$c_1 = (k_1 L)^2$ dan $c_2 = (k_2 L)^2$

$L$ adalah dynamic range citra (2bit – 1) dengan nilai default $k_1$ = 0.01 dan $k_2$ = 0.03. SSIM menggunakan perhitungan dari *Luminance* (***l***), *contrast* (***c***) dan *structure* (***s***) dimana bobot dari ketiga kriteria tersebut dianggap 1.

Dalam makalah ini telah dirangkum nilai enkripsi untuk masing-masing pesan pada SSIM dan PSNR. Hasil enkripsi pada citra cover dan file pesan dapat dilihat sebagai berikut:

**Tabel-2**. Perubahan Citra Setelah Proses Enkripsi

| Pesan (dalam byte) | Pesan Asli | Pesan Terenkripsi | SSIM | PSNR |
|---|---|---|---|---|
| 8 | del8apan | Óc□«öVŸ | 1 | 86.7532 |
| 16 | 16 enam belas 16 | å¯2□ý$«Š!Þ□ë÷^¥□ | 1 | 84.3228 |
| 32 | De Rosal, Ignatius Moses Setiadi | ?!{V£ªAOÕ*e¡ÏÇ:¤□ÅCŒ‰Q Ï0-Þ óË | 1 | 81.4883 |
| 64 | Image Steganography Technique using LSB and One Time Pads Cipher | s\x9iÇ□bp£gr-k‰Ýßa²M□Œ99h ‰ãX¨íÃ MÂ jq¸Öz □…¯èøt©□d□gÎ¸j • ÉZ )¤Ç | 1 | 78.2169 |
| 128 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM | ¡ðl~o□ÚØÿÎûO&+Fsˆ Qúì«³.Ä×} □×¬□“Tûd□ÏÞ:Çˆ/’□ ‹7ÑÛl(□øoÝ□ÈOpª¿ }•‘Ø%“ • Ù ÿóú¢ q M ,%ÒÎG¦9□Nv¨|ò©¹ • ¸Á à »¦ç.ãðUk-ÛÛ4>âËL□¡á:□g„G | 1 | 75.3005 |
| 256 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM | Ìªî»UÌÌÿªÝ»" ªÝ ÝÌª U"ªÿÿ ÿ"fUîÝªU»îD» 3Df " □wÝÝª UÌ»ÿDˆ»Ì w ÿwUÌ"3UÿÝf ÿÝÌ Ýf» 3Ìª»ÿU"ªî îÌ□U3D™□ | 1 | 72.1920 |
| 512 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM | Uª ªUÿªªÿ ÿU U ÿ ÿª Uÿ ÿÿUÿ ªÿªÿ ÿUªªU Uªª Uÿÿÿ ÿªUÿª Uª ÿ ÿÿÿª Uÿÿÿª ÿÿª ÿªU Uª Uÿÿ ª ªªUÿUªUU | 1 | 69.1670 |
| 1024 | Hiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEMHiding and Securing Message on Edge Areas of Image using Least Significant Bit Steganography and One Time Pads Encryption by CEM | ÿ ÿÿ ÿ ÿÿ ÿ ÿ ÿ ÿÿ ÿÿÿÿ ÿ ÿ ÿÿ ÿ ÿ ÿÿÿÿ ÿ ÿÿ ÿ ÿ ÿÿÿÿ ÿÿÿÿ ÿÿ ÿ ÿ ÿ ÿÿÿ ÿÿÿ ÿÿ | 0.9999 | 66.2075 |

Dari Tabel-2, dapat disimpulkan bahwa besarnya pesan yang disisipkan tidak terlalu mempengaruhi hasil enkripsi. Nilai SSIM untuk seluruh percobaan mendekati 1 dan nilai PSNR masih diatas 40 dB. Pembuktian proses enkripsi yang dilakukan sesuai pada potongan coding yang telah digunakan untuk eksperimen berikut ini.

```
[namafilepesan,pathpesan] =
uigetfile('*.txt','pilih pesan');
fileID = fopen(namafilepesan);
[pesan,panjangpesan] =
fread(fileID,inf,'uint8=>char');
fclose(fileID);
pesan1 = pesan';
kunci=109876;
fprintf('\n The message length is %d
\n', panjangpesan);
c=zeros(1,(panjangpesan*8));
ii=1;
iii=1;
if(mod(panjangpesan,8)==0)
    for(i=1:(panjangpesan/8))
        k=de2bi(kunci,56);
        str=pesan(ii:ii+7);
p=reshape(de2bi(double(str),8),[1 64]);
        c(iii:iii+63)=DES(p,'ENC',k);
        ii=ii+8;
        iii=iii+64;
    end
end
```

Untuk mengetahui waktu yang dibutuhkan dalam proses enkripsi dekripsi, dalam makalah ini penulis telah mereangkum dalam Tabel-2 dimana *software* yang digunakan yaitu Matlab 2015a, dengan RAM 8MB.

**Tabel-3.** Lama Waktu Enkripsi Dekripsi

| Pesan (dalam byte) | Enkripsi (dalam detik) | Dekripsi (dalam detik) |
|---|---|---|
| 8 | 0.414337 | 0.081110 |
| 16 | 0.488900 | 0.126241 |
| 32 | 0.604637 | 0.271466 |
| 64 | 0.887171 | 0.470710 |
| 128 | 1.365327 | 1.014022 |
| 256 | 2.409043 | 2.134284 |
| 512 | 2.421544 | 2.049057 |
| 1024 | 8.473227 | 7.502230 |

Dari Tabel 3, dapat disimpulkan bahwa lama waktu dekripsi DES pada media cover berupa gambar dan pesan berupa file .txt terbukti lebih cepat dibanding dengan enkripsinya.

## V. KESIMPULAN

Berdasarkan eksperimen yang telah dilakukan dapat disimpulkan bahwa performa DES dalam melakukan enkripsi gambar *grayscale* 512x512 dan pesan berupa teks panjang dapat dikategorikan dalam level yang baik. Skema DES yang digunakan dapat menghasilkan SSIM mendekati 1 dimana nilai SSIM 1 adalah sempurna. Pada proses enkripsi dan dekripsi, terjadi perbedaan waktu sesuai catatan waktu yang diilustrasikan pada Tabel 3. Sedangkan *imperceptibility* dianalisa melalui PSNR dengan perolehan nilai yang tinggi yaitu antara 66 sampai 86 dB.

## DAFTAR PUSTAKA

[1] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *Int. J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[2] A. Al-haj and H. Abdel-nabi, "Digital Image Security Based on Data Hiding and Cryptography," in *International Conference on Information Management Copyright*, 2017, pp. 437–440.

[3] Y. A. Gerhana, E. Insanudin, U. Syarifudin, and M. R. Zulmi, "Design of digital image application using vigenere cipher algorithm," in *2016 4th International Conference on Cyber and IT Service Management*, 2016, pp. 1–5.

[4] A. a. Shejul and U. L. Kulkarni, "A DWT Based Approach for Steganography Using Biometrics," in *2010 International Conference on Data Storage and Data Engineering*, 2010, pp. 39–43.

[5] E. J. Kusuma, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in *International Conference on Innovative and Creative Information Technology (ICITech)*, 2017, pp. 1–5.

[6] G. Ardiansyah, C. A. Sari, D. Setiadi, and E. H. Rachmawanto, "Hybrid Method using 3-DES , DWT and LSB for Secure Image Steganography Algorithm," in *International Conference on Information Technology, Information Systems, and Electrical Engineering*, 2017, pp. 248–253.

[7] J. K. M. S. U. Zaman and R. Ghosh, "Randomized DES Using Irreducible Polynomial Over Galois Field GF," *Int. J. Adv. Res. Comput. Sci.*, vol. 4, no. 10, pp. 760–766, 2013.

[8] D. P. Joseph and M. Krishna, "Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms," *Int. J. Adv. Res. Comput. Sci.*, vol. 6, no. 3, pp. 51–56, 2015.

[9] B. Prasetiyo, G. Rahmat, and N. Beta, "Kombinasi Steganografi Bit Matching dan Kriptografi DES untuk Pengamanan Data," *Sci. J. Informatics*, vol. 1, no. 1, pp. 79–93, 2014.

[10] S. Garg, S. Khera, and A. Aggarwal, "Extended Vigenere Cipher with Stream Cipher," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 5176–5180, 2016.

[11] M. B. Pramanik, "Implementation of Cryptography Technique using Columnar Transposition," pp. 19–23, 2014.

[12] D. R. I. M. Setiadi, A. E. Handoyo, E. H. Rachmawanto, C. A. Sari, and A. Susanto, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," *J. Teknol. dan Sist. Komput.*, vol. 6, no. 1, p. 37, Feb. 2018.

[13] M. a. Faizal, H. B. Rahmalan, E. H. Rachmawanto, and C. A. Sari, "Impact Analysis for Securing Image Data using Hybrid SLT and DCT," *Int. J. Futur. Comput. Commun.*, vol. 1, no. 3, pp. 309–311, 2012.

[14] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[15] A. Hore and D. Ziou, "Image Quality Metrics: PSNR vs. SSIM," in *2010 20th International Conference on Pattern Recognition*, 2010, pp. 2366–2369.