

# **Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar**

Ifan Rizqa<sup>\*1)</sup>, Aprilyani Nur Safitri<sup>2)</sup>, Imanuel Harkespan<sup>3)</sup>

\*Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro  
<sup>1)</sup>risqa.ifan@dsn.dinus.ac.id, <sup>2)</sup>aprilyani.safitri@dsn.dinus.ac.id, <sup>3)</sup>harkespan@dsn.dinus.ac.id

## **Abstrak**

*Aplikasi yang menerapkan metode LSB dan algoritma kriptografi DES ini berjalan dengan baik dan mampu menyisipkan dan mengekstrakan pesan dan dapat mengenkripsi dan deskripsi isi pesan. Pada penelitian Penyisipan Pesan Ke Dalam Gambar Dengan Menggunakan Metode Least Significant Bit (LSB) dan enkripsi dengan menggunakan Algoritma Data Encryption Standard (DES) yang mempunyai tujuan untuk menambah keamanan pesan agar seseorang yang tidak bertanggung jawab tidak dapat mengetahui sebuah pesan rahasia yang akan dikirim. Aplikasi ini hanya mengamankan sebuah pesan kedalam sebuah citra dan merubah isi pesan dari yang dikethai maknanya ke yang tidak diketahui maknanya. Pada penelitian ini telah diterapkan metode LSB-DES pada gambar 281x320 pixel dengan cover berupa gambar berwarna dan pesan berupa kata. PSNR yang dihasilkan adalah 86.64 db untuk pesan kata “rahasia”. Berdasarkan penelitian dapat disimpulkan hasil PSNR nilainya tinggi, maka kualitas citra bagus, maka dari itu hasil gambar steganografi pun sangat baik.*

**Kata kunci :** DES, Enkripsi, LSB, citra berwarna

## **Abstract**

*Applications that apply the LSB method and the DES cryptographic algorithm are running well and are able to insert and extract messages and can encrypt and describe the contents of messages. In the study of Inserting Messages into Images Using the Least Significant Bit (LSB) method and encryption using the Data Encryption Standard (DES) Algorithm which has the aim of increasing message security so that someone who is not responsible cannot know a secret message to be sent. This application only secures a message into an image and changes the message content from the known meaning to the unknown meaning. In this study, the LSB-DES method has been applied to a 281x320 pixel image with a cover in the form of a color image and a message in the form of words. The resulting PSNR is 86.64 db for the word “rahasia”. Based on the research, it can be concluded that the PSNR value is high, so the image quality is good, therefore the results of the steganography image are also very good..*

**Keywords :** DES, Encryption, LSB, color image

## 1 PENDAHULUAN

Dalam era globalisasi dan perkembangan teknologi saat ini, banyak cara atau teknik untuk melindungi informasi rahasia agar orang lain yang tidak mempunyai hak tidak dapat mengakses informasi tersebut. Untuk melindungi informasi banyak teknik yang bisa digunakan seperti steganografi [1].

Steganografi yaitu suatu teknik yang dapat menyisipkan pesan kedalam citra digital seperti gambar, video, dan teks, dengan kapasitas data yang disisipkan direpresentasikan dalam bentuk bit per pixel [2]. Citra asli yang digunakan untuk menyisipkan data disebut *cover-image*, dan gambar yang telah disisipkan data disebut *stego-image*. Distorsi pada *stego-image* dapat diukur menggunakan *peak signal-to-noise ratio* (PSNR) [3].

Penelitian ini menggunakan Last Significant Bit (LSB), cara ini menyediakan kapasitas yang sangat besar dalam penyimpanan pesan dan memiliki kualitas pada citra yang sangat baik. Kombinasi kriptografi dan steganografi dapat meningkatkan keamanan data. Salah satu metode kriptografi untuk pengamanan data adalah Data Encryption Standard (DES) [4]. Algoritma ini telah banyak diterapkan untuk proses enkripsi di mesin ATM dan operator kartu SIM di seluruh dunia [5].

Berdasarkan kelebihan penggunaan Data Encryption Standard (DES) dengan digabungkannya metode Least Significant Bit (LSB), maka penelitian ini mengusulkan kombinasi antara kriptografi untuk menyandikan pesan dan steganografi untuk penyisipan pesan rahasia kedalam gambar, agar pesan tidak bisa dibaca oleh seseorang yang tidak mempunyai hak atas pesan tersebut.

Hasil yang ingin dicapai dari penelitian ini adalah penggunaan metode Data Encryption Standard (DES) dan metode Least Significant Bit (LSB) yang mampu menghasilkan PSNR yang lebih baik. Juga, melindungi informasi rahasia dan penting dari orang lain agar penerimaan informasi aman dan terjaga secara *real-time*.

## 2 TINJAUAN PUSTAKA

### 2.1 STEGANOGRAFI

Ilmu yang menyembunyikan suatu informasi dengan cara memasukan informasi tersebut ke dalam suatu pesan lain merupakan pengertian dari steganografi [6]. Tujuan dari steganografi adalah menyembunyikan informasi tersebut agar informasi tidak dapat diketahui oleh orang lain. Steganografi juga merupakan pelengkap dari kriptografi [7]. Perbedaan steganografi dan kriptografi adalah jika dalam steganografi pesan disembunyikan sedemikian rupa sehingga orang lain tidak dapat mengetahui pesan tersebut [8]. Jika dalam kriptografi pesan diubah menjadi karakter aneh maka dalam steganografi pesan disembunyikan dalam sebuah media. Media tersebut dapat berupa media digital seperti musik, teks maupun gambar [9].

### 2.2 DES

Salah satu algoritma yang digunakan dalam kriptografi untuk menjaga keamanan suatu data dengan cara mengenkripsinya sehingga data tersebut aman dan hanya bisa dibuka jika

dengan menggunakan kunci merupakan algoritma enkripsi DES (*Data Encryption Standard*) [10].

Algoritma ini merupakan algoritma yang sering digunakan. Algoritma ini diadopsi oleh NIST (National Institute of Standards and Technology) sebagai standar pengolahan informasi Federal AS. Plain dienkrip dalam blok-blok 64 bit menjadi 64 bit data ciphertext menggunakan kunci 56 bit kunci internal (*internal key*) [11]. DES merupakan block cipher karena mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Algoritma DES digunakan untuk membalik enkripsi [12]. Dengan menggunakan 56 bit kunci internal (*internal key*) atau up-kunci (*subkey*) DES mengenkripsikan 64 bit plaintext menjadi 64 bit ciphertext [13].

### 2.3 LSB

Salah satu teknik substitusi steganografi adalah metode LSB (*Least Significant Bit*). Dimana tiap bit terendah pada byte-byte media citra akan digantikan dengan bit-bit pesan yang akan disisipkan. Terdapat susunan tiga warna, yaitu merah, hijau dan biru (*RGB*) yang masing-masing disusun oleh bilangan 8 bit (1 *byte*) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111 pada file citra 24 bit setiap pixel pada citra [14]. Metode ini menggunakan citra digital sebagai *cortex* sehingga lebih sederhana dan mudah untuk diimplementasikan [15].

### 2.4 PENELITIAN TERKAIT

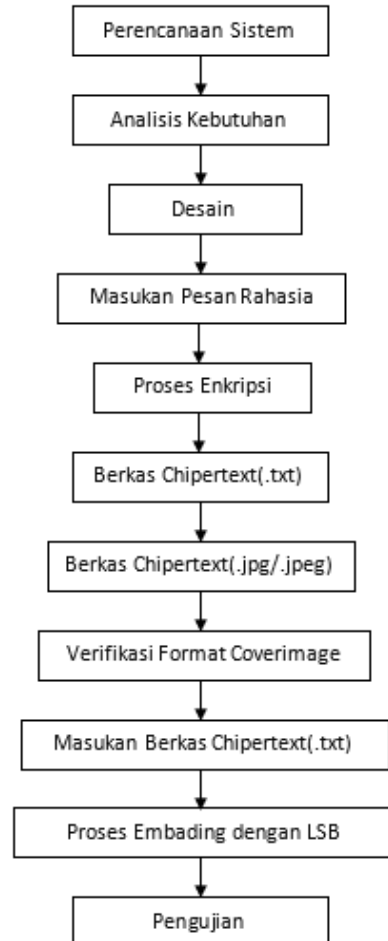
Terkait dengan penelitian ini, berikut adalah penelitian terkait yang telah dilakukan sebelumnya sebagai referensi penulis. Penelitian yang telah dilakukan meliputi pada Tabel 1.

**Tabel 1 State of The Art**

No	Nama Peneliti	Judul Penelitian	Hasil
1	Tseng, Hsien-Wen dan Leng, Hui-Shih	A Steganographic Method Based on Pixel Value Differencing and the Perfect Square Number	Hasil percobaan menunjukkan skema yang diusulkan memberikan kapasitas besar dan imperseptibilitas yang tinggi.
2	V, Nadiya P dan Imran, B Mohammed	Image Steganography in DWT Domain using Double-Stegging with DES	Mode-1 menggunakan Double Stegging dengan pengkodean RSA terbukti jauh lebih efisien.
3	Moumen, Abdelkader dan Sissaoui, Hocine	Images Encryption Method using Steganographic LSB Method, AES and RSA algorithm	Diperoleh kualitas dari gambar akhir yang baik (PSNR > 50 dB) dan memiliki ketahanan terhadap noise.
4	Paulus Lucky Tirma Irawan, Budi Purnomo, Oesman Hendra Kelana	Rancang Bangun Aplikasi Manajemen hak Cipta Citra Digital Menggunakan DES Dan LSB	Nilai rerata yang tinggi dari pengujian MSE terhadap citra stegano sebesar 0,371. Sementara untuk komponen nilai PNSR didapatkan rerata nilai sebesar 121,045
5	Edi Jaya Kusuma, Christy Atika Sari, Oktaviana Rena Indriani, Eko Hari Rachmawanto, De Rosal Ignatius Moses Setiadi	An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption	Nilai MSE ( <i>Mean Square Error</i> ) dan PSNR ( <i>Peak to Noise Ratio</i> ) memperoleh rata-rata nilai terbaik MSE sebesar 0,0038557 dan nilai PSNR 72.2698 dB.

### 3 METODE PENELITIAN

Penelitian ini menggunakan kombinasi dari Algoritma DES dan LSB untuk dikembangkan kedalam sebuah sistem pengamanan pesan. Dalam pengembangan sistem, penelitian ini menggunakan proses seperti yang diperlihatkan pada Gambar 1.



Gambar 1 Alur Pengembangan Sistem

#### 3.1 PERENCANAAN SISTEM

Pertama, dalam sistem yang akan dibuat adalah cara mengirim pesan rahasia yang aman dan tidak terlihat mencurigakan serta meningkatkan keamanan pada pesan, sehingga orang yang lain tidak menyadari bahwa ada pesan rahasia yang sedang dikirim. Berdasarkan permasalahan yang ada, maka dibuatlah sistem penyandian pesan secara rahasia menggunakan metode kriptografi DES kemudian menanamkan pesan rahasia yang sudah disandikan ke bentuk media gambar menggunakan metode *Least Significant Bit* (LSB).

#### 3.2 DESAIN

Bentuk diagram merupakan alur dari sistem dan proses penggambaran yang akan dibuat. Tujuan dari sistem diagram adalah menggambarkan tentang model diagram yang ada pada alur sistem nantinya dibentuk nyata pada sistem di tahap implementasi. Sistem diagram digunakan

untuk membantu proses implementasi yaitu *use casediagram*, *activity diagram*, dan *sequence diagram*.

### 3.3 IMPLEMENTASI

Penerapan kombinasi dari metode kriptografi DES dan metode steganografi Least Significant Bit (LSB) merupakan implementasi dari penelitian ini, agar mendapat keamanan tinggi untuk mengamankan pesan rahasia agar sampai tujuan dengan utuh dan aman. Pada implementasi tersebut format file yang digunakan pada penyisipan berkas ciphertext adalah (.txt), sedangkan format file yang digunakan pada cover image yang disebut sebagai wadah adalah (.jpeg/.jpg). Untuk mendapatkan pesan rahasia atau plaintext dengan cara, pertama memasukan stegoimage dari hasil proses penyisipan demi mendapatkan berkas ciphertext, kemudian berkas ciphertext di deskripsi, cara tersebut merupakan proses ekstraksi berkas.

### 3.4 TAHAPAN EKSTRAKSI DAN PENYISIPAN PESAN

Proses ekstraksi dan penyisipan pesan adalah sebagai berikut:

1. Memasukan Pesan Rahasia  
Pengirim memasukan pesan kedalam sistem agar dapat diberi sandi untuk menjaga kerahasiaanya.
2. Proses Enkripsi  
Proses penyamaran pesan menggunakan metode kriptografi DES.
3. Melakukan Input Cover Image  
Gambar yang akan dimasukan kedalam sistem sebagai media penampung nantinya menjadi cover image baru memiliki format (.jpeg/.jpg).
4. Melakukan Input Berkas Ciphertext  
Format (.txt) merupakan format berkas ciphertext yang nantinya sipengirim akan menyisipkan kedalam cover image
5. Verifikasi Cover Image dan Berkas Ciphertext  
Cover image harus berformat(.jpeg/.jpg), dan ciphertext diharuskan mempunyai format (.txt) agar proses verifikasi menjaga kekonsistenan pada hasil stegoimage
6. Proses Penyisipan Berkas  
Pengirim menyisipkan berkas dengan menggunakan metode steganografi Least Significant Bit (LSB) didalamnya mengandung pesan rahasia. Format yang stegoimage adalah (.png) karena mempunyai akurasi baik dalam penyimpanan data (lossless).

### 3.5 TAHAPAN EKSTRAKSI DAN DESKRIPSI

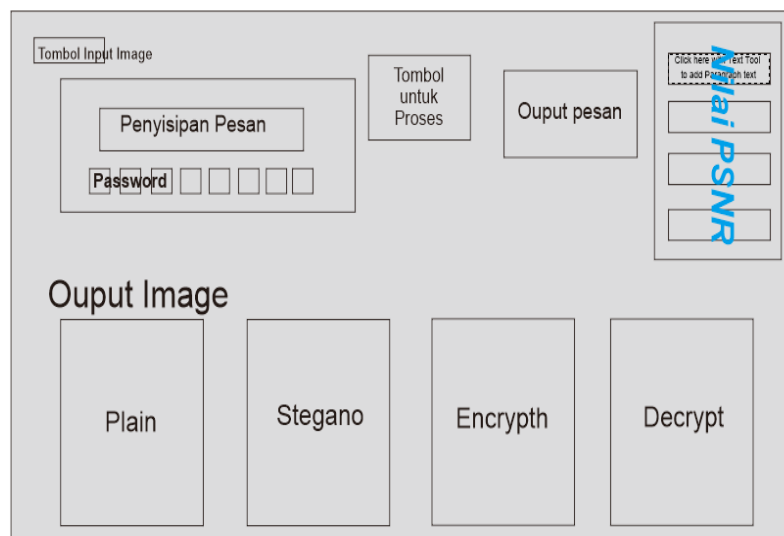
Proses ekstraksi sampai deskripsi si penerima melakukan berbagai tahapan seperti berikut :

1. Melakukan input storage  
Setelah mendapatkan stegoimage dari sipengirim, sipenerima memasukan stegoimage ke sebuah sistem.
2. Verifikasi stegoimage  
Sistem melakukan proses verifikasi pada stegoimage guna mengetahui mungkinkah format stegoimage dimasukan sipenerima mempunyai format (.png) atau tidak.

3. Proses ekstraksi  
Metode steganografi Least Significant Bit (LSB) yang digunakan untuk proses pengembalian berkas menjadi output berbentuk berkas ciphertext.
4. Input berkas ciphertext  
Sebagai proses dekripsi, sipenerima memasukan berkas chphertext dari hasil ekstraksi kedalam sistem.
5. Proses dekripsi  
Untuk mengembalikan dari bentuk ciphertext menjadi pesan rahasia (plaintext), penerima melakukan proses deskripsi yang dilakukan oleh sistem menggunakan metode kriptografi DES
6. Tahapan enkripsi dan dekripsi  
Proses enkripsi ini membuktikan bahwa pesan bisa kembali ke bentuk asli tanpa memodifikasi, dan mengurangi isinya.

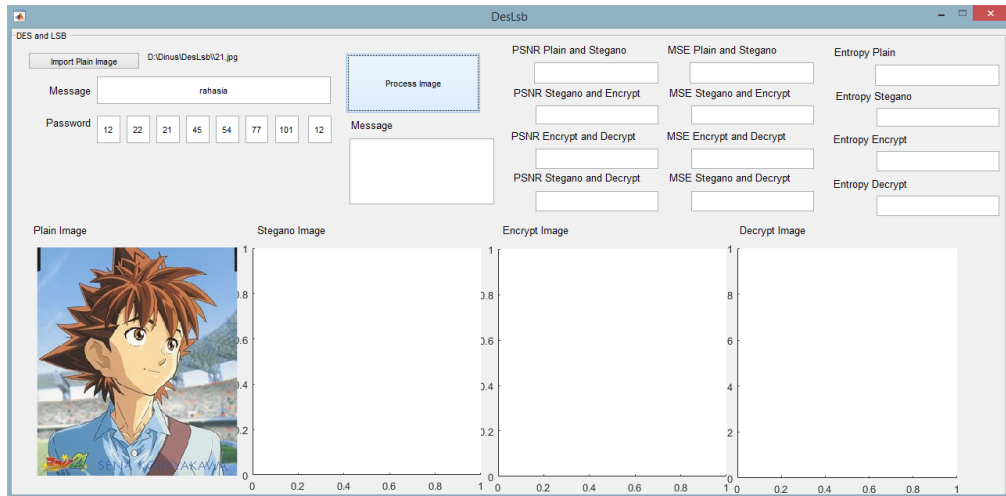
#### 4 HASIL DAN PEMBAHASAN

Dalam implementasi pengaplikasian program kali ini menggunakan perangkat lunak matlab R2015b, untuk memudahkan penulis melakukan penelitian untuk menyisipkan pesan ke dalam gambar yang ber format (.jpg) dengan menggunakan Data Encryption Standard (DES) dan metode Least Significant Bit (LSB).



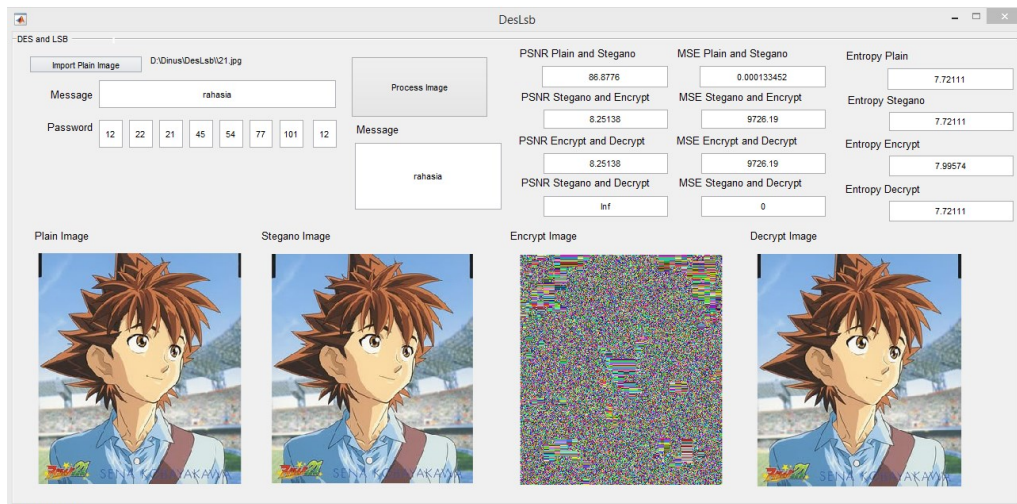
**Gambar 2 Desain Program**

Pada gambar 2, merupakan desain pada program sebelum dibuat program selanjutnya pada matlab, agar memudahkan penulis untuk mem proses pembuatan program selanjutnya, sehingga tidak repot untuk harus bagaimana tampilan program nantinya.



**Gambar 3 Realisasi Program**

Pada gambar 3 merupakan realisasi program pada matlab yang kurang lebih sesuai mockup/desain sebelumnya dengan sedikit kembangan sehingga dapat nyaman digunakan serta dipahami yang menilai, terdapat bebarapa fitur dalam tampilan. Fitur dalam tampilan program merupakan seperti tombol terdapat 2 tombol yang digunakan untuk meng input gambar dan tombol lainnya untuk memproses gambar untuk di sisipkan pesan serta password yang nantinya menjadi output gambar dan juga nilai PSNR, MSE, Entropy.











**Gambar 4 Tampilan Akhir**

Pada gambar 4 merupakan contoh tampilan akhir proses dengan hasil gambar tertampil lengkap dan juga nilai PSNR, MSE, Entropy dalam proses pemasukan pesan serta password pada gambar berformat (.jpg) yang dimasukkan, dengan ini proses pada program sudah selesai.

Berikut hasil pengujian berupa ukuran file sebelum dan sesudah encode, PSNR, MSE entropy berhasil setidaknya proses penyisipan dan ekstraksi untuk menghasilkan isi pesan yang disisipkan.

**Tabel 2 Hasil Pengujian**

<b>Nama File</b>	<b>Ukuran Pixel</b>	<b>Ukuran Cover Image</b>	<b>PSNR Plan Stegano</b>	<b>MSE</b>	<b>Entropy</b>	<b>Berhasil/Tidak</b>
 <b>21.jpg</b>	281x320	31kb	86,87db	0,000133	7,721	Berhasil
 <b>Eight.jpg</b>	252x288	8kb	85,59db	0,000179	1,913	Berhasil
 <b>Hydrangeas.jpg</b>	1024x768	581kb	96,42db	0,000144	9,712	Berhasil
 <b>Jellyfish.jpg</b>	1024x768	757kb	98,05db	0,00121	9.882	Berhasil
 <b>Koala.jpg</b>	1024x768	762kb	86,67db	0,00054	9,625	Berhasil
 <b>Lighthouse.jpg</b>	1024x768	548kb	96,41db	0,000341	6,721	Berhasil
 <b>M1.jpg</b>	960x545	68kb	96,11db	0,000103	3,256	Berhasil
 <b>Penguins.jpg</b>	1024x768	759kb	96,17db	0,000192	11,243	Berhasil

Gambar 5 menampilkan contoh hasil pada program untuk mengetahui hasil pada proses dengan mengetahui nilai PSNR pada suatu gambar setelah di enkripsi.



PSNR Plain and Stegano	MSE Plain and Stegano	Entropy Plain
86.8776	0.000133452	7.72111
PSNR Stegano and Encrypt	MSE Stegano and Encrypt	Entropy Stegano
8.25138	9726.19	7.72111
PSNR Encrypt and Decrypt	MSE Encrypt and Decrypt	Entropy Encrypt
8.25138	9726.19	7.99574
PSNR Stegano and Decrypt	MSE Stegano and Decrypt	Entropy Decrypt
inf	0	7.72111

Gambar 5 Nilai PSNR pada gambar yang sudah dienkripsi

## 5 KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut:

1. Aplikasi yang menerapkan metode LSB dan algoritma kriptografi DES ini berjalan dengan baik mampu menyisipkan dan mengekstrakan pesan, dan dapat mengenkripsi dan deskripsi isi pesan.
2. Pada penelitian Penyisipan Pesan Ke Dalam Gambar Dengan Menggunakan metode Least Significant Bit (LSB) dan enkripsi dengan menggunakan Algoritma Data Encryption Standard (DES) yang mempunyai tujuan untuk menambah keamanan pesan agar seseorang yang tidak bertanggung jawab tidak dapat mengetahui sebuah pesan rahasia yang akan dikirim.
3. Aplikasi ini hanya mengamankan sebuah pesan kedalam sebuah citra dan merubah isi pesan dari yang diketahui maknanya ke yang tidak diketahui maknanya.
4. Pada penelitian ini telah diterapkan metode LSB-DES pada gambar 281x320 pixel dengan cover berupa gambar berwarna dan pesan berupa kata. PSNR yang dihasilkan adalah 86,64 db, MSE yang dihasilkan adalah 0,000133 , Nilai Entropy yang dihasilkan adalah 7,721 untuk pesan kata “rahasia”. Berdasarkan penelitian dapat disimpulkan hasil PSNR nilainya tinggi, maka kualitas citra bagus, maka dari itu hasil gambar steganografi pun sangat baik, hasil MSE nilainya semakin kecil mendekati dengan 0 maka nilai kemiripan dan kualitas citra dapat dikategorikan bagus.

## DAFTAR PUSTAKA

- [1] I. Gunawan, “Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video,” *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 57, 2018, doi: 10.30645/j-sakti.v2i1.48.
- [2] Y. B. Utomo and D. Erwanto, “Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor,” *Gener. J.*, vol. 3, no. 1, p. 16, 2019, doi: 10.29407/gj.v3i1.12698.
- [3] I. Gunawan, Sumarno, E. Irawan, and H. S. Tambunan, “Pengamanan Berkas Dokumen Menggunakan Fungsi Algoritma Steganografi LSB,” *Algoritm. J. Ilmu Komput. dan Inform.*, vol. 02, no. 01, pp. 61–65, 2018.
- [4] M. Winafil, S. Sinurat, and T. Zebua, “KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer) IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD DAN TRIPLE DATA ENCRYPTION STANDARD

- UNTUK MENGAMANKAN CITRA DIGITAL,” vol. 2, pp. 450–459, 2018, [Online]. Available: <http://ejurnal.stmik-budidarma.ac.id/index.php/komik>.
- [5] “ATTACK AND OPTIMIZING SECURITY MANAGEMENT ON ATM MACHINES USING.”
- [6] S. R. Widiyanto, “Desain dan Analisa Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) ...,” *J. Elektra*, vol. 3, no. 1, pp. 37–46, 2018, [Online]. Available: <https://pei.ejournal.id/jea/article/view/44>.
- [7] S. R. Widiyanto, “Desain Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) Yang Tahan Terhadap Gangguan,” *Pros. Semin. Nas. Sains dan Teknol.*, pp. 1–8, 2018.
- [8] CA. Sari, EH. Rachmawanto, " Gabungan Algoritma Vernam Chiper dan End of File Untuk Keamanan Data", *Techno. Com*, Vol. 13, no. 3, pp. 150-157, 2014.
- [9] Y. Fatma, H. Mukhtar, and M. Taufik, “Implementasi Steganografi Pada Teks Terenkripsi Dengan Algoritma Rsa Menggunakan Metode Bpcs,” *J. Fasilkom*, vol. 7, no. 2, pp. 260–265, 2018, doi: 10.37859/jf.v7i2.783.
- [10] N. Syahputri, “Rancang Bangun Aplikasi Kriptografi Pengamanan Transmisi Data Multimedia Menggunakan Algoritma Data Encryption Standard,” *Maj. Ilm. Methoda*, vol. 9, no. 2, pp. 57–63, 2019.
- [11] N. R. Yanti, A. Alimah, and D. A. Ritonga, “Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database,” *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 23, 2018, doi: 10.30645/j-sakti.v2i1.53.
- [12] A. Prameshwari and N. P. Sastra, “Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen,” *Eksplora Inform.*, vol. 8, no. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.
- [13] A. Adil Yazdeen, S. R. M. Zeebaree, M. Mohammed Sadeeq, S. F. Kak, O. M. Ahmed, and R. R. Zebari, “FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review,” *Qubahan Acad. J.*, vol. 1, no. 2, pp. 8–16, 2021, doi: 10.48161/qaj.v1n2a38.
- [14] H. Fonda, “Klasifikasi Batik Riau Dengan Menggunakan Convolutional Neural Networks (Cnn),” *J. Ilmu Komput.*, vol. 9, no. 1, pp. 7–10, 2020, doi: 10.33060/jik/2020/vol9.iss1.144.
- [15] A. Hafis, “Steganografi Berbasis Citra Digital untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB),” *J. Cendikia*, vol. XVII, no. April, pp. 194–198, 2019.