ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.3 No.1 Tahun 2024
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024
Fakultas Teknik, Universitas Pelita Bangsa, Januari 2024

Implementasi Penyembunyian Pesan pada Citra dengan Menggabungkan Algoritma Caesar Cipher dan Metode LSB

Implementation of Message Concealment in Images by Combining Caesar Cipher Algorithm and LSB Method

Silvia Delya Heryani[1], Ade Maulani Bilgis[2], Modesta Liunesi[3]

[123]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa

[1]silviadelyaheryani31@gmail.com, [2]ademaulanibilgiss@gmail.com*, [3]modestaliunesi@gmail.com*

Abstract

In today's digital era, information security is becoming increasingly important given the increasing threats to data confidentiality. This research aims to combine two methods, namely the Caesar Cipher algorithm encryption method and the LSB (Least Significant Bit) algorithm method, in an effort to increase the security of messages hidden in the image. Caesar Cipher is used to encrypt the message before it is inserted into the image, while the LSB (Least Significant Bit) method is used to hide the message in less significant bits in the image pixels.

This research applies a practical approach by integrating both techniques in an efficient and effective system. In addition, the quality of the image in which the message is inserted is evaluated to ensure that the modifications do not significantly reduce the visual quality of the image.

The experimental results show that combining the Caesar Cipher algorithm encryption method and the LSB (Least Significant Bit) algorithm method is able to provide a higher level of security than using the LSB (Least Significant Bit) algorithm method alone. Therefore, this approach can be considered as a potential solution to enhance the security of messages in images without significantly compromising the visual quality of the image. The practical implementation of this research can be applied in various contexts, such as secure communication and exchange of confidential information in the digital domain.

Keywords: *Caesar Cipher, LSB (Least Significant Bit), Cryptography*

Abstrak

Dalam era digital saat ini, keamanan informasi menjadi semakin penting mengingat meningkatnya ancaman terhadap kerahasiaan data. Penelitian ini bertujuan untuk menggabungkan dua metode, yaitu metode enkripsi algoritma *Caesar Cipher* dan metode algoritma LSB *(Least Significant Bit)*, dalam upaya meningkatkan keamanan pesan yang disembunyikan pada citra. *Caesar Cipher* digunakan untuk mengenkripsi pesan sebelum disisipkan ke dalam citra, sementara metode LSB *(Least Significant Bit)* digunakan untuk menyembunyikan pesan tersebut pada bit-bit yang kurang signifikan pada piksel citra.

Penelitian ini menerapkan pendekatan praktis dengan mengintegrasikan kedua teknik tersebut dalam sebuah sistem yang efisien dan efektif. Selain itu, dilakukan evaluasi terhadap kualitas citra hasil penyisipan pesan untuk memastikan bahwa modifikasi tidak mengurangi kualitas visual citra secara signifikan.

Hasil eksperimen menunjukkan bahwa penggabungan metode enkripsi algoritma *Caesar Cipher* dan metode algoritma LSB *(Least Significant Bit)* mampu memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan penggunaan metode algoritma LSB *(Least Significant Bit)* saja. Oleh karena itu, pendekatan ini dapat dianggap sebagai solusi yang potensial untuk meningkatkan keamanan pesan pada citra tanpa mengorbankan kualitas visual citra secara berarti. Implementasi praktis dari penelitian ini dapat diterapkan dalam berbagai konteks, seperti komunikasi aman dan pertukaran informasi rahasia dalam domain digital.

***Kata kunci**: Caesar Cipher, LSB (Least Significant Bit*), *Kriptografi*

Pendahuluan

Pesatnya perkembangan teknologi saat ini, telah muncul beragam metode untuk melindungi pesan atau informasi yang perlu dijaga kerahasiaannya dari potensi ancaman seperti pencurian data dan upaya peretasan. Maka dari itu, untuk menghambat upaya pihak yang tidak bertanggung jawab terhadap kejahatan komputer, penulis mengusulkan penggabungan antara kriptografi, khususnya algoritma *Caesar Cipher* [1] untuk mengenkripsi pesan, dan steganografi dengan menggunakan metode LSB *(Least Significant Bit)* [2] guna meningkatkan tingkat keamanan pesan. Saat ini, berbagai teknik telah dikembangkan untuk menjaga keamanan data dan informasi, termasuk di dalamnya kriptografi [3] dan steganografi [4]. Steganografi adalah seni menyisipkan pesan rahasia ke dalam suatu media, memungkinkan pesan tersebut tetap tidak berubah bentuknya, terutama saat disisipkan pada citra digital, sehingga orang lain tidak dapat mendeteksi keberadaan pesan rahasia tersebut. Salah satu metode steganografi yang diadopsi dalam penelitian ini adalah metode LSB *(Least Significant Bit)*, yang melibatkan penggantian bit data yang kurang signifikan pada segmen citra dengan bit-bit rahasia yang tertanam pada bit terakhir [5]. Sedangkan, kriptografi adalah ilmu yang berkaitan dengan teknik enkripsi di mana data diacak menggunakan kunci enkripsi, sehingga sulit dibaca oleh pihak yang tidak memiliki kunci deskripsi [6]. Penelitian ini mengaplikasikan algoritma *Caesar Cipher* sebagai metode enkripsi sederhana yang berbasis pergeseran huruf. Dengan fokus pada implementasi penyembunyian pesan pada citra digital, penulis akan menjelaskan lebih rinci mengenai penggabungan algoritma *Caesar Cipher* dan metode LSB *(Least Significant Bit)*.

Metode Penelitian

Pengumpulan Data Citra

Pengumpulan data citra uji yang akan digunakan untuk menguji metode penyembunyian pesan merupakan langkah penting dalam pengembangan sistem steganografi. Data citra uji ini digunakan untuk menguji seberapa efektif dan aman metode penyembunyian pesan yang telah dikembangkan. Proses pengumpulan data citra uji dapat dilakukan dengan beberapa langkah sebagai berikut:

a. Pemilihan Citra
   Memilih citra yang representatif dan bervariasi untuk dijadikan sebagai data uji. Citra-citra ini sebaiknya mencakup berbagai jenis, resolusi, dan karakteristik untuk memastikan keberagaman dalam pengujian.
b. Sumber Citra
   Memastikan legalitas sumber citra yang akan diuji untuk metode penyembunyian pesan.
c. Preprocessing
   Melakukan preprocessing pada citra-citra uji. Hal ini dapat mencakup normalisasi resolusi, konversi format file, atau pembersihan citra dari noise atau artefak yang tidak diinginkan.
d. Metadata
   Mengumpulkan metadata dari citra-citra uji tersebut, seperti informasi tentang kamera, tanggal pengambilan gambar, dan lain sebagainya. Hal ini dapat membantu dalam analisis dan pengujian lebih lanjut.

Setelah data citra uji terkumpul, langkah selanjutnya adalah menguji metode penyembunyian pesan yang telah dikembangkan menggunakan citra-citra tersebut.

Implementasi Algoritma *Caesar Cipher*

Algoritma *Caesar Cipher* adalah metode sederhana untuk mengenkripsi pesan dengan melakukan pergeseran karakter sesuai dengan kunci tertentu. Langkah-langkah implementasi algoritma *Caesar Cipher* untuk mengenkripsi pesan adalah sebagai berikut:

a. Konversi Pesan ke Dalam Angka
   Konversi setiap karakter dalam pesan ke dalam nilai numerik sesuai dengan urutan alfabet. Misalnya, huruf "A" menjadi 0, "B" menjadi 1, dan seterusnya.
b. Pergeseran Karakter
   Lakukan pergeseran terhadap nilai numerik setiap karakter sesuai dengan kunci enkripsi yang telah ditentukan. Misalnya, jika kunci enkripsi adalah 3, maka setiap nilai numerik akan digeser sebanyak 3. Jika hasil pergeseran melebihi 25, maka kembali ke awal alfabet.
c. Konversi Kembali ke Karakter
   Konversikan kembali nilai numerik yang telah diubah ke dalam karakter sesuai dengan alfabet. Misalnya, nilai 0 menjadi "A", nilai 1 menjadi "B", dan seterusnya.

Implementasi Metode LSB

Metode LSB *(Least Significant Bit)* adalah metode steganografi yang digunakan untuk menyisipkan pesan rahasia ke dalam citra digital. Proses ini melibatkan penggantian bit-bit paling tidak signifikan (LSB) dari piksel-piksel dalam citra dengan bit-bit pesan yang akan disisipkan [7]. Proses ini biasanya dilakukan pada citra berwarna atau grayscale. Langkah-langkah implementasi metode LSB untuk menyisipkan pesan yang telah dienkripsi ke dalam citra adalah sebagai berikut:

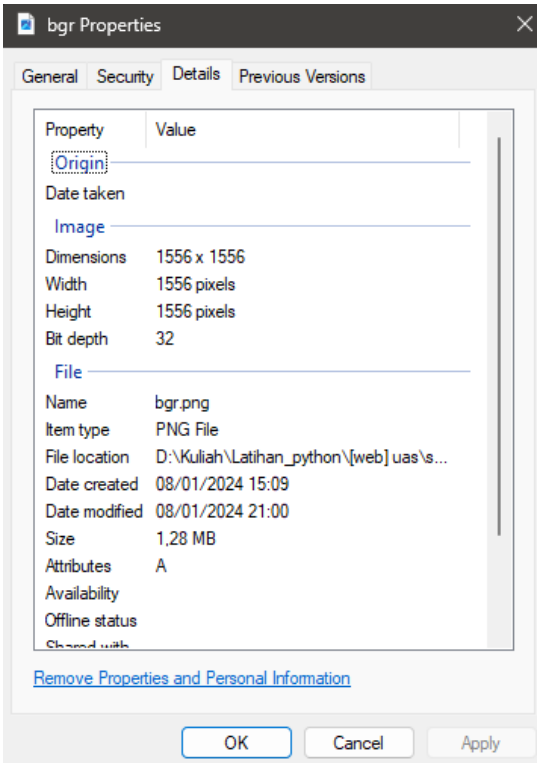
1. Enkripsi Pesan
   Pesan yang akan disisipkan ke dalam citra perlu dienkripsi terlebih dahulu menggunakan algoritma enkripsi yang aman, seperti AES [8] atau RSA [9]. Hal ini untuk memastikan keamanan pesan yang disisipkan.
2. Pemilihan Piksel
   Pilih piksel-piksel dalam citra yang akan digunakan untuk menyimpan bit-bit pesan. Piksel-piksel ini biasanya dipilih secara acak atau berdasarkan algoritma tertentu agar penyisipan pesan tidak terlalu terlihat.
3. Konversi Pesan ke Bit
   Pesan yang telah dienkripsi kemudian dikonversi ke dalam urutan bit-bit yang akan disisipkan ke dalam citra.
4. Penyisipan Pesan
   Bit-bit pesan yang telah dienkripsi kemudian disisipkan ke dalam LSB dari setiap saluran warna (RGB) atau saluran grayscale dari piksel-piksel yang telah dipilih.
5. Analisis keamanan
   Menganalisis keamanan terhadap pesan yang disisipkan dengan menggunakan algoritma *Caesar Cipher*.

Algoritma *Caesar Cipher* adalah metode enkripsi sederhana yang menggeser setiap huruf dalam teks sejauh nilai tetap dalam abjad. Analisis keamanan terhadap pesan yang disandikan dengan *Caesar Cipher* dapat dilakukan dengan beberapa metode. *Caesar Cipher* hanya memiliki 25 kemungkinan pergeseran (karena 26 pergeseran akan

mengembalikan pesan ke keadaan aslinya), maka metode *brute force* dapat digunakan untuk mencoba semua kemungkinan pergeseran dan melihat mana yang menghasilkan pesan.

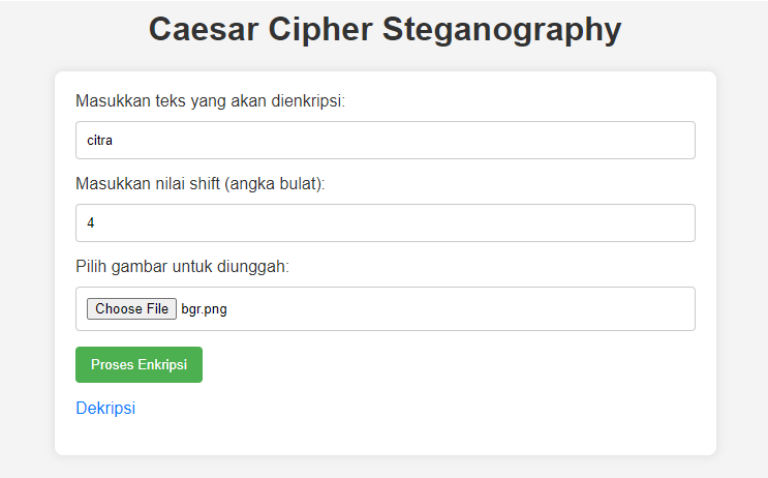
Hasil dan Pembahasan

Pada penelitian ini pengujian dilakukan pada objek berupa citra digital grayscale dengan format PNG yang kemudian dilakukan penyandian dan penyisipan pesan teks. Pesan hasil enkripsi dari *Caesar Cipher* akan disisipkan ke dalam citra grayscale. Detail ukuran citra sebelum dilakukan penyisipan pesan sebesar 1,28 MB dengan dimensi piksel sebesar 1556 x 1556, dapat dilihat pada gambar 1.



Gambar 1 Detail Citra Awal

Implementasi penelitian ini menggunakan bahasa pemrograman *python* [10] dengan menggunakan framework Flask, sehingga untuk melakukan pengujian dapat dilakukan dengan tampilan layar web. Pada tampilan awal aplikasi ini dijalankan, akan muncul halaman utama yang berisi tiga form, yaitu form untuk memasukkan teks yang akan dienkripsi, form untuk memasukkan nilai shift (pergeseran), dan form untuk menggunggah citra digital yang akan disisipkan pesan. Dapat dilihat pada gambar 2.



Gambar 2 Halaman Utama

Proses ini menggunakan teknik steganografi dengan memanfaatkan nilai piksel pada citra. Pesan yang akan kami sisipkan adalah 'citra' yang akan di enkripsi dengan metode *Caesar Cipher*. Pergeseran sebanyak empat karakter dipilih sebagai kunci enkripsi. Setiap huruf dalam kata 'citra' digeser empat langkah ke depan dalam alfabet. Seperti pada tabel di bawah ini:

Tabel 1 Pergeseran Empat Karakter

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Pesan yang akan kami sisipkan adalah 'citra', maka hasilnya huruf 'c' menjadi 'g', huruf 'i' menjadi 'm', huruf 't' menjadi 'x', huruf 'r' menjadi 'v', huruf 'a' menjadi 'e'. Maka enkripsinya menjadi 'gmxve'. Formalnya, enkripsi *Caesar Cipher* dapat dijelaskan dengan rumus matematika:

$$E(x) = (x + n)\ mod\ 26$$

Dengan keterangan, E(x) adalah fungsi enkripsi untuk karakter x, sedangkan n adalah jumlah langkah pergeseran, dan mod 26 mengindikasikan bahwa kita menghitung hasil modulo 26 untuk memastikan karakter tetap dalam rentang alfabet [11].

Pesan sudah terenkripsi, selanjutnya akan diubah menjadi pesan enkripsi ke dalam bentuk biner, dimana setiap karakter diubah menjadi urutan 8 bit sesuai dengan ASCII [12] seperti pada tabel di bawah ini:

Tabel 2 Nilai ASCII dan Biner

Enkripsi	Kode ASCII	Biner
g	103	01100111
m	109	01101101
x	120	01111000
v	118	01110110
e	101	01100101

Pesan yang telah terenkripsi akan disisipkan ke dalam citra menggunakan metode LSB *(Least Significant Bit)*. Konsep utama dari metode LSB *(Least Significant Bit)* adalah menyisipkan pesan atau data rahasia dengan mengganti bit-bit yang paling tidak berarti dari data yang sudah ada, karena perubahan pada bit paling tidak berarti umumnya memiliki dampak yang paling kecil pada data asli, perubahan ini dapat menjadi sulit untuk terdeteksi secara visual. Seperti perubahan bit di bawah ini:

00100101 → 00100100

Pada tabel 3 di bawah ini, merupakan nilai biner awal pada citra uji sebelum disisipkan pesan. Bit pada biner ini akan diubah menggunakan metode LSB *(Least Significant Bit)*. Setelah bit-bit pada biner diubah dengan metode LSB *(Least Significant Bit)* hasilnya seperti pada tabel 4.

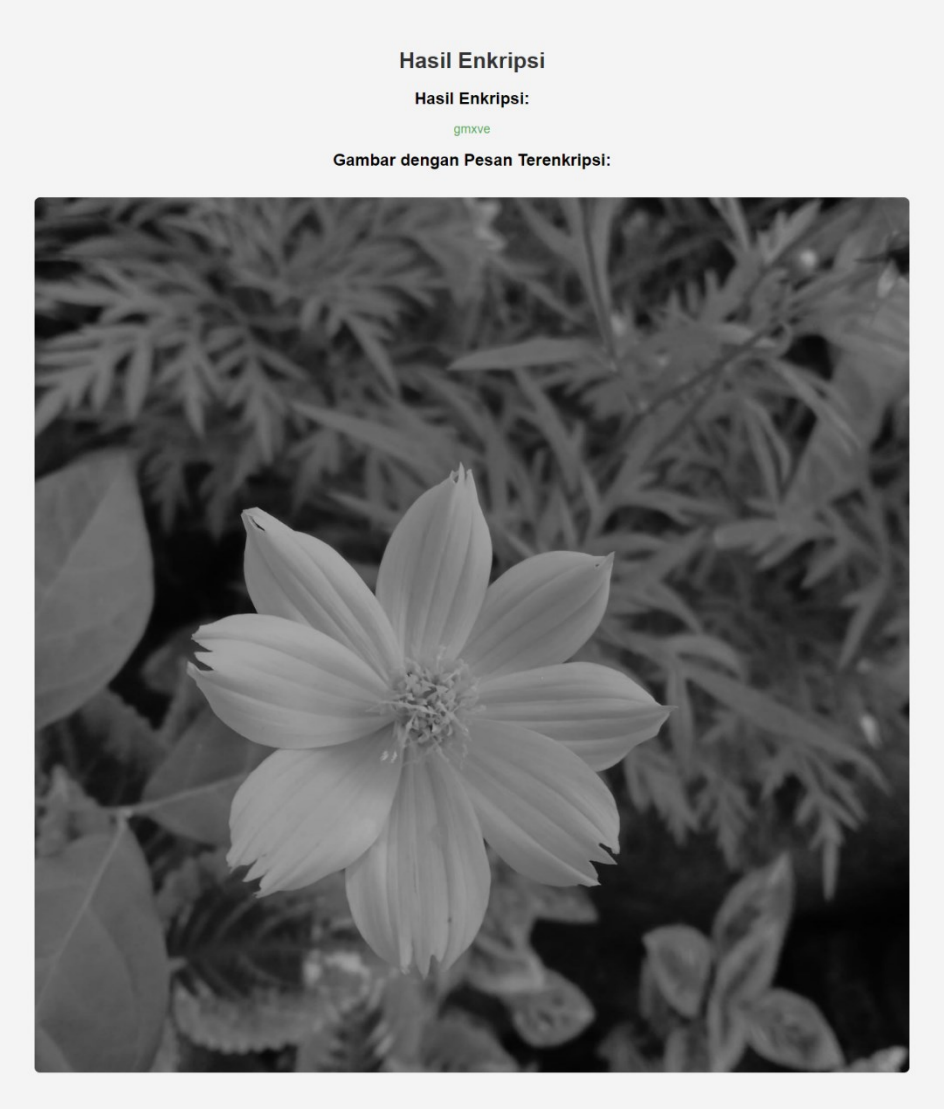
Tabel 3 Nilai Biner Awal

00100101	00100100	00100100	00100100	00100011	00100011	00100011	00100011	00100100	00100101
00100101	00100101	00100101	00100101	00100101	00100101	00100101	00100101	00100111	00100111
00100110	00100110	00100110	00100110	00100111	00100111	00101000	00101000	00101010	00101010
00100110	00100110	00100111	00101000	00101001	00101010	00101010	00101011	00101101	00101101
00100101	00100101	00100111	00101000	00101001	00101011	00101100	00101100	00101110	00101111
00100011	00100100	00100101	00100111	00101001	00101011	00101100	00101101	00101110	00101110
00100001	00100001	00100011	00100101	00101000	00101010	00101100	00101101	00101101	00101101
00011111	00100000	00100010	00100100	00100111	00101001	00101011	00101100	00101100	00101100
00100000	00100001	00100010	00100011	00100101	00100110	00101000	00101000	00101101	00101110
00100001	00100010	00100011	00100011	00100101	00100110	00100111	00101000	00101100	00101110

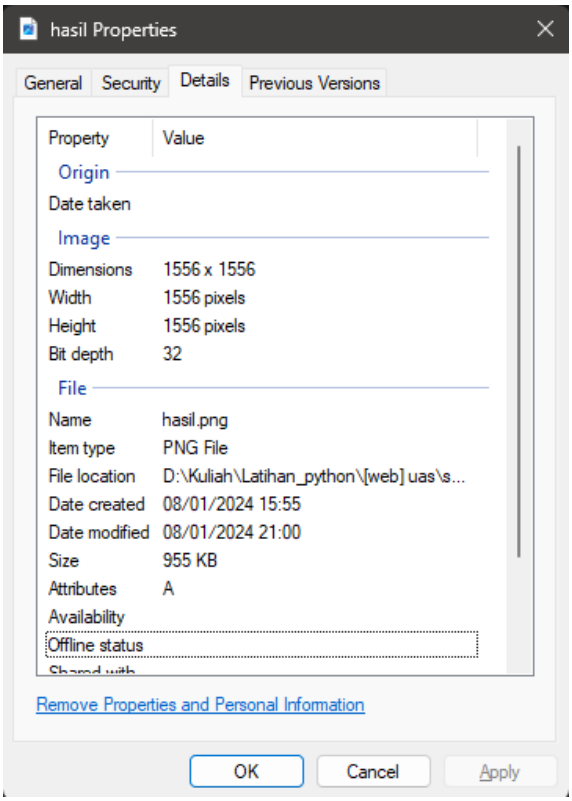
Tabel 4 Nilai Biner Hasil

00100100	00100101	00100100	00100100	00100011	00100010	00100011	00100011	00100100	00100100
00100101	00100101	00100101	00100101	00100101	00100101	00100101	00100101	00100111	00100111
00100110	00100110	00100110	00100110	00100111	00100111	00101000	00101000	00101010	00101010
00100110	00100110	00100111	00101000	00101001	00101010	00101010	00101011	00101101	00101101
00100101	00100101	00100111	00101000	00101001	00101011	00101100	00101100	00101110	00101111
00100011	00100100	00100101	00100111	00101001	00101011	00101100	00101101	00101110	00101110
00100001	00100001	00100011	00100101	00101000	00101010	00101100	00101101	00101101	00101101
00011111	00100000	00100010	00100100	00100111	00101001	00101011	00101100	00101100	00101100
00100000	00100001	00100010	00100011	00100101	00100110	00101000	00101000	00101101	00101110
00100001	00100010	00100011	00100011	00100101	00100110	00100111	00101000	00101100	00101110

Proses selanjutnya setelah melakukan enkripsi, aplikasi akan menampilkan halaman hasil enkripsi *Caesar Chiper* dan metode LSB, dapat dilihat pada gambar 3. Citra awal yang telah disisipkan pesan dengan algoritma *Caesar Chiper* dan metode LSB, terjadi perubahan pada ukuran citra hasil sebesar 955 KB dan dimensi piksel yang tidak berubah sebesar 1556 x 1556, terlihat pada gambar 4.



Gambar 3 Halaman Hasil Enkripsi



Gambar 4 Detail Citra Hasil

Pesan yang telah terenksripsi dan disisipkan ke dalam citra dengan menggunakan metode LSB *(Least Significant Bit)*, akan dilakukan analisis untuk menginterpretasi dampak dari penyembunyian pesan terhadap kualitas citra. Dalam tahap ini, penulis menggunakan metrik-metrik seperti PSNR [13] dan MSE [14] untuk mengukur kualitas citra, sehingga kita dapat mengevaluasi sejauh mana pesan dapat disembunyikan tanpa mengorbankan kualitas visual secara signifikan [15].

Tabel 5 Detail Citra Awal dan Hasil

Detail Citra	Citra Awal	Citra Hasil
Nama citra	bgr.png	hasil.png
Ukuran	1,28 MB	955 KB
Dimensi (Piksel)	1556 x 1556	1556 x 1556

Pada tabel 5 merupakan detail citra yang diujikan, citra awal dengan nama bgr.png memiliki ukuran sebesar 1,28 MB dengan dimensi (piksel) sebesar 1556 x 1556. Setelah citra disisipkan pesan, citra hasil dengan nama hasil.png berubah ukurannya yang semula 1,28 MB menjadi 955 KB dengan dimensi (piksel) yang masih sama seperti citra awal sebelum disisipkan pesan. Secara visual, citra yang belum disisipkan pesan pada gambar 5 dan citra yang telah disisipkan pesan pada gambar 6, tidak terlihat perubahan yang signifikan.

Gambar 5 Citra Awal

Gambar 6 Citra Hasil

Untuk mengetahui kulaitas citra yang telah disisipkan pesan, maka kami akan menganalisis citra menggunakan metrik PSNR *(Peak Signal-to-Noise Ratio)* dan MSE *(Mean Squared Error)* untuk mendapatkan indikasi kualitas citra hasil sisipan.

Tabel 6 PSNR dan MSE

PSNR	MSE
101.97 dB	4.13e-06

Pada tabel di atas hasil MSE menunjukan seberapa kecil kesalahan rata-rata kuadrat antara citra asli dan citra hasil yang sudah disisipkan pesan, sementara PSNR memberikan informasi tentang seberapa baik citra hasil jika dibandingkan dengan citra asli, diukur dalam satuan desibel, nilai PSNR yang tinggi dan MSE yang rendah umumnya mengindikasikan bahwa perbedaan antara kedua citra relatif kecil, dan citra hasil memiliki kualitas yang baik.

Kesimpulan

Berdasarkan penelitian terhadap aplikasi penyembunyian pesan pada citra digital dengan menggabungkan metode algoritma *Caesar Cipher* dan metode LSB *(Least Significant Bit)*, maka dapat disimpulkan bahwa tidak terdapat perubahan yang berarti pada hasil citra, baik sebelum maupun setelah disisipkan pesan. Citra hasil setelah disisipkan pesan tergolong baik dengan nilai PSNR adalah sebesar 101.97 dB. Secara visual, perbedaan citra asli dan citra hasil hampir tidak dapat terlihat.

Daftar Rujukan

[1] Rihartanto, Didi Susilo Budi Utomo, and Ansar Rizal, "Implementasi Image Tilling Pada Penyembunyian Pesan Menggunakan LSB," *Proceeding SINTAK*, pp. 186-192, 2019.

[2] Angga Aditya Permana and Habib Amna, "Implementasi Steganografi File Citra Digital Menggunakan Metode Least Significant Bit", *Jurnal Teknik*, 2022, vol. 11, no. 01, pp. 62-72, Jun. 2022.

[3] Maya Sari, Hindriyanto Dwi Purnomo, and Irwan Sembiring, "Algoritma Kriptografi Sistem Keamanan SMS di Android", Jurnal Information Technology, Vol. 2, No. 1, Mar. 2022.

[4] Yesi Puspita Dewi, "Pengembangan Teknik Steganografi dengan Kriptografi Modifikasi dari Caesar Cipher dan SHA-256 untuk Merahasiakan Pesan", *Jurnal Ilmu Komputer dan Desain Komunikasi Visual*, vol. 5. no. 1. pp. 10-21, Jul. 2020.

[5] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb)", *Jurnal Cendikia*, vol. 17, no. 1 April, pp. 194-198, Apr. 2019.

[6] Fitri Yanti and Khairi Budayawan, "Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb) dalam Pengamanan Informasi pada Citra Digital", *Jurnal Vocational Teknik Elektronika dan Informatika*, vol. 11, no. 1, pp. 63 – 70, 2023.

[7] Aditya Aziz Fikhri and Hendrawaty, "Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android", *Jurnal Infomedia*, vol. 3, no. 1, Jun. 2018.

[8] Ajib Susanto and Ibnu Utomo Wahyu Mulyono, "Kombinasi LSB-RSA Untuk Peningkatan Imperceptibility Pada Kripto-Stegano Gambar RGB", *Proceeding SENDIU*, pp. 21 – 27, 2020.

[9] Irvan Maulana Yusup, Carudin, and Intan Purnamasari, "Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen", *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 6, no. 3, pp. 434 – 441, 2020. http://dx.doi.org/10.28932/jutisi.v6i3.2817

[10] A. F. Humaira, R. Marwati, and K. Yulianti, "Implementasi Kriptografi Secret Sharing Scheme dan Steganografi Audio Least Significant Bit (LSB)", *JMT (Jurnal Matematika dan Terapan)*, vol. 5, no. 1, pp. 1 – 11, 2023. https://doi.org/10.21009/jmt.5.1.1

[11] Rindy Febrianingsih and Aliy Hafiz, "Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data", *Jurnal Informasi Dan Komputer*, vol. 7, no. 2, pp. 81 – 86, 2019.

[12] Priyagung Hernawandra, Supriyadi, and U. Tresna Lenggana, "Aplikasi Steganografi Menggunakan LSB 4 Bit Sisipan dengan Kombinasi Algoritme Substitusi dan Vigenere Berbasis Android", *Jurnal Teknologi dan Sistem Komputer*, vol. 6, no. 2, pp. 44 – 50, 2018. 10.14710/jtsiskom.6.2.2018.44-50

[13] Rika Humayrah, Andi Marwan Elhanafi, and M. Taufik Batubara, "Analisa Histogram dan PSNR Pada Citra True Color Dalam Pengamanan Teks Menggunakan Spread Spectrum dan LSB", *Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI)*, vol. 2, no. 1, pp. 188 – 200, 2023.

[14] Firda Kurniasih, Rini Marwati, and Ririn Sispiyati, "Penggabungan Affine Cipher dan Least Significant Bit 2 untuk Penyisipan Pesan Rahasia pada Gambar", *Jurnal EurekaMatika*, vol. 11, no.2, pp. 79 – 88, 2023.

[15] Dimas Yoga Pramuda, "Analisa Pengujian Kualitas Citra Steganografi Dengan Pendekatan Parameter PSNR Dan MSE", *Prosiding SNASTIKOM*, pp. 233 – 241, 2021.