ISSN : 2723 - 4193
E-ISSN : 2775-8338

ANALISIS IMPLEMENTASI STEGANOGRAFI DENGAN ALGORITMA DES UNTUK MENGATASI MODIFIKASI CITRA DIAM *(FOTO)*

Syahrul Mustafa[1], Umar Muhammad[2], Rocky Djumu[3]

Teknik Listrik Politeknik Bosowa[12]

Teknik Elektro Universitas Muslim Indonesia[3]

Jalan Kapasa Raya no. 23 Kima, Daya Kode Pos 90241, Makassar, Sulawesi Selatan
Jalan Urip Sumoharjo Km5 Kode Pos 90231, Makassar, Sulawesi Selatan
Syahrulmustafa@politeknikbosowa.ac.id[1], Umar.muhammad@politeknikbosowa.ac.id[2]

Abstrak

Beberapa teknik perlindungan terhadap manipulasi digital di atas yang telah populer sejak Perang Dunia II dan telah mengalami banyak perkembangan pesat saat ini seperti Kriptografi, Steganografi dan *watermarking*. hasil pengujian proses steganografi citra digital yang dimofikasi. Citra pesan yang digunakan berupa citra digital *.bmp. Pengujian dilakukan dengan menyisipkan tiga citra pesan yang memiliki ukuran berbeda-beda untuk melihat pengaruh proses penyisipan pesan terhadap perubahan nilai pixel, histogram serta nilai MSE dan PSNR. hasil analisis penggunaan steganografi dengan algoritma DES dan fungsi hash untuk mengatasi modifikasi citra, dengan menggunakan citra Banana.bmp, Treasuremap.bmp, dan Twins.bmp sebagai citra pesan, serta citra Monalisa.bmp sebagai citra penampung. Implementasi Algoritma DES dan Fungsi Hash pada teknik steganografi menghasilkan citra steganografi yang memiliki *robustness* terhadap modifikasi citra yang diujikan antara lain *fog, invert, mirror, lighten, darken.* Semakin kecil ukuran citra pesan yang disisipkan maka semakin baik citra staganografi yang dihasilkan. Banana.bmp dengan ukuran 245 KB memiliki MSE sebesar 1,263E-03 dan PSNR sebesar 38,559 dB. Treasuremap.bmp dengan ukuran 195 KB memiliki MSE sebesar 8,957E-04 dan PSNR sebesar 39,305 dB. Twins.bmp dengan ukuran 195 KB memiliki MSE sebesar 2,809E-04 dan PSNR sebesar 41,822 dB
Kata Kunci: Steganografi, Algoritma Des, Fungsi Hash

Abstract

Some of the protection techniques against digital manipulation above have been popular since World War II and have experienced many rapid developments today, such as Cryptography, Steganography and watermarking. results of testing the modified digital image steganography process. The message image used is a digital image *.bmp. Testing was carried out by inserting three message images of different sizes to see the effect of the message insertion process on changes in pixel values, histograms and MSE and PSNR values. results of analysis of the use of steganography with the DES algorithm and hash function to overcome image modification, using the Banana.bmp, Treasuremap.bmp, and Twins.bmp images as message images, and the Monalisa.bmp image as a container image. Implementation of the DES Algorithm and Hash Function in steganography techniques produces steganographic images that have robustness to the image modifications tested, including fog, invert, mirror, lighten, darken. The smaller the size of the message image inserted, the better the staganographic image produced. Banana.bmp with a size of 245 KB has an MSE of 1.263E-03 and a PSNR of 38.559 dB. Treasuremap.bmp with a size of 195 KB has an MSE of 8.957E-04 and a PSNR of 39.305 dB. Twins.bmp with a size of 195 KB has an MSE of 2.809E-04 and a PSNR of 41.822 Db
Keywords: **Steganografi, Algoritma Des, Hash Function**

1. Pendahuluan

Kehidupan modern saat ini tidak lepas dari kemajuan teknologi digital. Misalnya transaksi di mesin ATM, transaksi di bank, transaksi dengan kartu kredit, percakapan melalui telepon genggam, mengakses internet, mengaktifkan peluru kendali, tanda tangan digital, pengolahan suara digital , pengolahan video digital, pengolahan gambar/citra digital dan lain sebagainya. Semua kegiatan di atas sudah sangat umum dan rentan dengan manipulasi digital seperti pembajakan, pencurian, pelanggaran hak cipta konten media dan lain sebagainya [1][2][3]. Beberapa teknik perlindungan terhadap manipulasi digital di atas yang telah populer sejak Perang Dunia II dan telah mengalami banyak perkembangan pesat saat

ISSN : 2723 - 4193
E-ISSN : 2775-8338

ini seperti Kriptografi, Steganografi dan watermarking.

Pada prinsipnya ketiga teknik yang telah disebutkan di paragraf sebelumnya adalah sama yaitu menyisipkan sesuatu berupa pesan/data ke dalam pesan/data yang lain, tetapi tujuan dari ketiganya berbeda. Kriptografi bertujuan menyembunyikan /menyisipkan pesan pada suatu media agar isi pesan tidak bisa dibaca oleh selain penerima pesan. Steganografi bertujuan menyembunyikan/menyisipkan pesan pada suatu media agar pesan tidak bisa diketahui oleh selain penerima pesan. Watermarking bertujuan menyembunyikan /menyisipkan pesan pada suatu media agar media yang disisipi bisa dipastikan keasliannya oleh penerima pesan[4], [5].

Pada laporan tugas akhir yang menjadi referensi penulisan laporan ini, telah dibahas tentang steganografi menggunakan metode enkripsi CBC (Cipher Block Chain) dan LSB (Least Significant Bit) untuk metode penyisipan pesannya. Data steganografi yang dihasilkan mampu bertahan dari gangguan AWGN (Additive White Gaussian Noise)[6][7].

Dalam kasus steganografi pada tugas akhir ini adalah pesan/data disisipkan pada citra digital dan harus memenuhi sifat ketahanan (robustness). Ketahanan yang dimaksud adalah pesan/data yang disisipkan tidak terpengaruh dari upaya untuk menghilangkan atau merusak pesan/data tersebut baik sengaja atau tidak sengaja. Serangan (attack) terhadap pesan/data meliputi simple attack, detection disabling, removal dan ambiguity[8][3]. Modifikasi pada citra meliputi foging, inverting, mirror, lighten, darken, rotating, addition, croping, resizing, scaling dan lain-lain dapat juga membuat kerusakan pada pesan atau data tersebut.

Masalah ini sangatlah penting dalam steganografi karena pesan/data hasil steganografi tahan terhadap serangan maupun modifikasi sehingga pesan/data yang disisipkan dapat diungkapkan kembali seperti aslinya. Untuk itu diperlukan teknik steganografi yang memiliki ketergantungan terhadap arsip penampungnya. Ketergantungan ini meningkatkan keamanan pesan/data yang disisipkan karena untuk melakukan pengungkapan pesan/data diperlukan arsip penampung yang asli sebagai verfikasi. Salah satu cara yang umum untuk memperoleh ketergantungan tersebut adalah dengan menggunakan Algoritma DES (Data Encryption Standard) dan Fungsi Hash (MD5) sebagai metode enkripsi.

2. Metode

Perancangan bertujuan agar dalam pembuatan program dapat berjalan secara sistematis, terstruktur, dan terarah sehingga hasil program dapat optimal dan berjalan sesuai dengan apa yang dikehendaki. Dalam perancangan, yang perlu diperhatikan adalah kemampuan program, efektifitas, efisiensi, dan kemudahan untuk dipahami pengguna (user friendly) yang diwujudkan dalam tampilan grafis (Graphical User Interface)[9].

2. 1 Spesifikasi Sistem

Berikut ini diberikan pada tabel II-1 spesifikasi dari peralatan-peralatan utama yang digunakan.

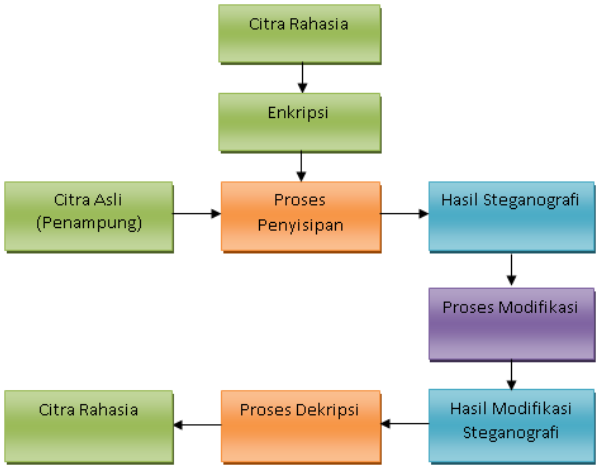
Tabel 1. Spesifikasi Perangkat yang digunakan dalam penelitian Tugas Akhir

Jenis Perangkat	Spesifikasi
Processor	Intel® Core ™ i3-2367M CPU @ 1.40 GHz
Memory	4096 MB
Hard disc	500 GB
Sistem Operasi	Windows 7
Bahasa Pemrograman	Visual Basic 6.0

2.2 Diagram Blok Sistem

Diagram blok sistem secara umum dapat digambarkan pada gambar 1.

ISSN : 2723 - 4193
E-ISSN : 2775-8338



Gambar 1. Diagram blok sistem

Pada penulisan skripsi ini, program dibuat dalam sebuah sistem yang terdiri dari beberapa blok dengan fungsi yang spesifik. Diagram blok sistem menggambarkan proses kerja sistem mulai dari masukan sampai keluaran, yang dapat dijelaskan secara umum sebagai berikut :

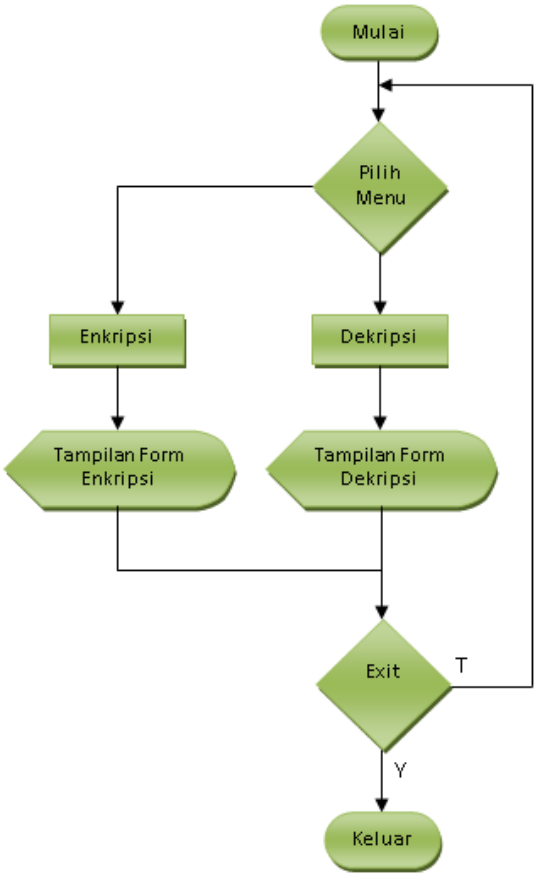
1. Citra digital dengan format bitmap 24 bit disiapkan sebagai penampung data rahasia yang akan disisipkan.
2. Pesan rahasia atau disebut juga dengan *plaintext* terlebih dahulu di enkripsi untuk memberikan jaminan integritas dan kerahasiaan informasi, metode enkripsi yang digunakan adalah *Data Encryption Standard* (DES) dan fungsi hash (MD5). Hasil enkripsi disebut dengan *ciphertext.*
3. Proses selanjutnya adalah penggantian bit-bit pada berkas penampung (berupa citra digital dengan format bitmap 24 bit) dengan bit-bit *ciphertext*. Keluaran dari proses ini disebut dengan hasil steganografi.
4. Hasil steganografi kemudian disimulasikan dengan berbagai proses modifikasi.
5. Hasil steganografi yang telah mengalami proses modifikasi akan didekripsi. Proses dekripsi ini berfungsi untuk mengambil *ciphertext* yang terkandung dalam hasil steganografi. Hasil proses dekripsi yaitu *plaintext* atau pesan rahasia yang semula disembunyikan.

2.3 Perancangan Diagram Alir

Perancangan diagram alir dimaksudkan untuk menggambarkan urutan dan tahap pembuatan program serta memperjelas penggunaannya. Perancangan diagram alir program terdiri atas perancangan diagram alir menu utama, program enkripsi dan program dekripsi.

2.3.1 Perancangan Diagram Alir Menu Utama

Diagram alir menu utama menggambarkan urutan penggunaan program dengan menu-menu yang tersedia, yang menghubungkan ke pilihan-pilihan yang akan ditampilkan. Diagram alir menu utama program analisis pengunaan steganografi denagn algoritma DES dan fungsi Hash untuk mengatasi modifikasi citra ditunjukkan pada Gambar 2.



Gambar 2. Diagram Alir Menu Utama

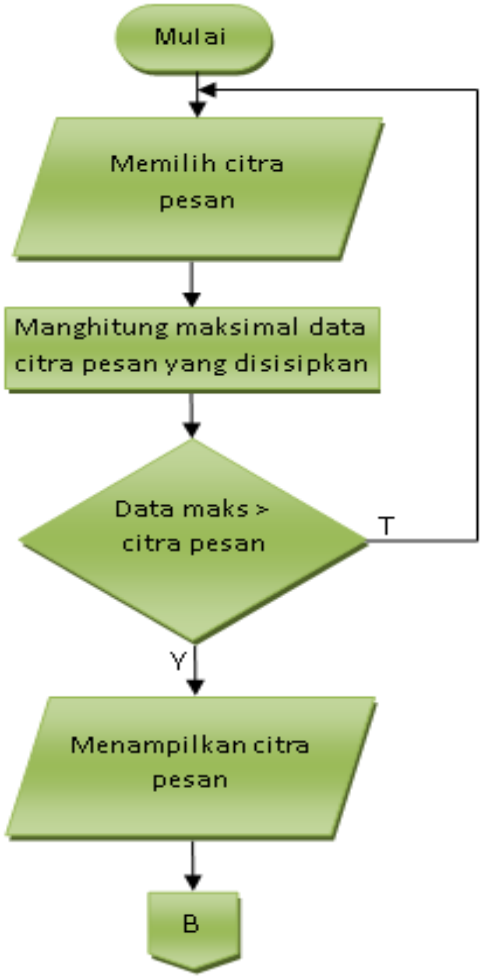
Pada Gambar 2 dapat dijelaskan bahwa pada saat program dijalankan akan ditampilkan menu utama pada *form* **Menu Utama** yang terdiri atas tiga pilihan menu yang bisa dipilih untuk ditampilkan. Pilihan menu tersebut terdiri atas pilihan ***Enkripsi*** untuk masuk ke *form* ***Enkripsi*** (proses

ISSN : 2723 - 4193
E-ISSN : 2775-8338

penyembunyian data), pilihan **Dekripsi** untuk masuk ke *form* **Dekripsi** (proses pengungkapan data) dan pilihan **Keluar** yaitu untuk keluar dari program.

2.3.2 Perancangan Diagram Alir Program Enkripsi

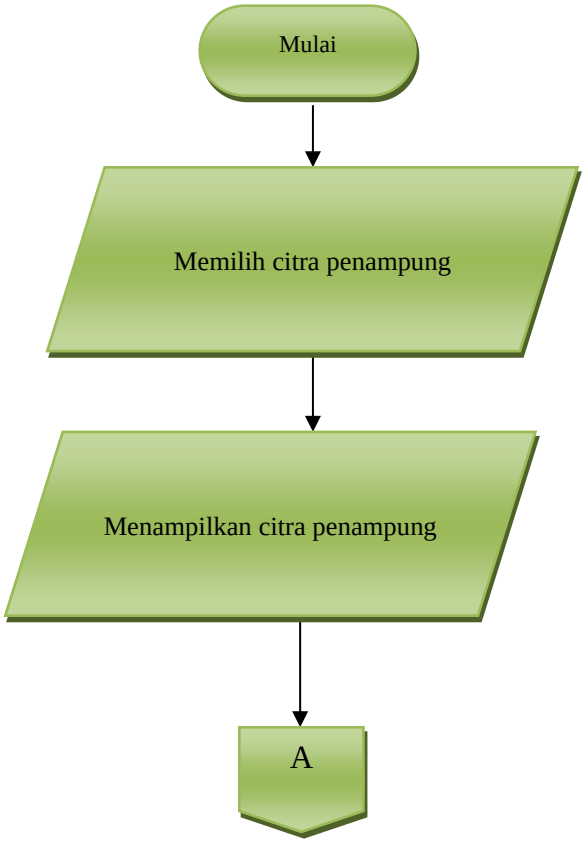
Diagram alir program enkripsi menggambarkan urutan penggunaan menu yang tersedia pada *form* ***Enkripsi***. Diagram alir program enkripsi terbagi menjadi beberapa bagian yang saling berhubungan.
Untuk bagian yang pertama adalah diagram alir pengambilan citra yang digunakan sebagai berkas penampung, seperti yang terlihat pada Gambar 3.



Gambar 3. Diagram alir memilih citra penampung

Pada Gambar 3 terlihat bahwa proses dimulai dengan memilih citra penampung. Citra penampung yang akan dipilih berformat bitmap. Citra penampung yang telah dipilih akan ditampilkan pada *form*.

Bagian yang kedua adalah diagram alir untuk proses pemilihan citra yang akan disisipkan, seperti yang terlihat pada Gambar 4.

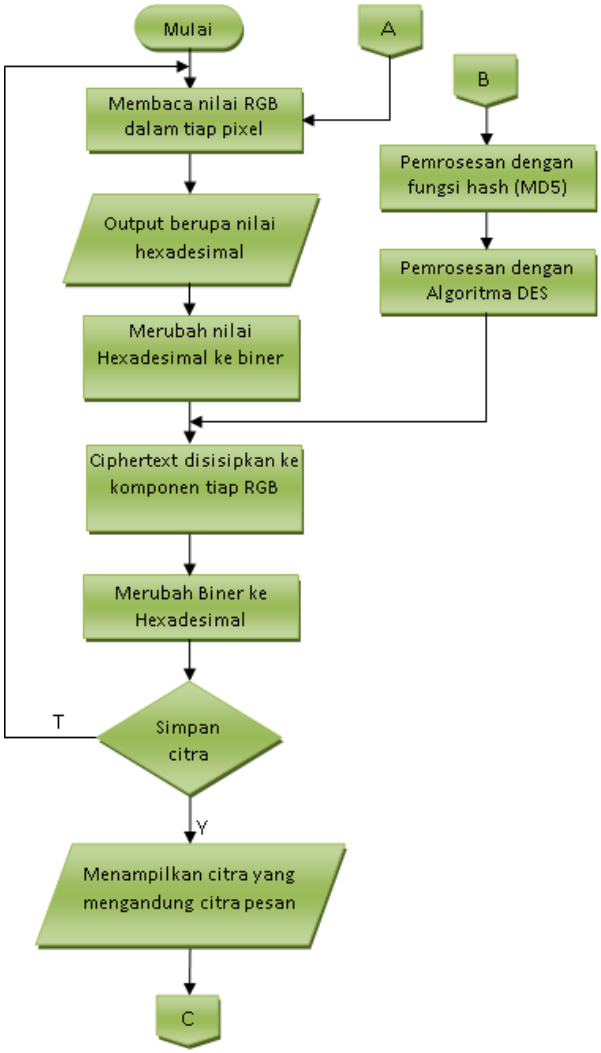


Gambar 4. Diagram alir memilih citra pesan yang disisipkan

Pada Gambar 4 terlihat proses pemilihan citra pesan. Citra pesan yang akan disisipkan berformat bitmap. Setelah dipilih, maka program akan menghitung ukuran citra pesan. Jika daya tampung maksimal lebih besar dari ukuran citra pesan yang akan disisipkan maka citra pesan akan ditampilkan pada form.

Bagian yang ketiga adalah diagram alir proses penyisipan citra pesan steganografi menggunakan fungsi hash (MD5) dan algoritma DES. Diagram alirnya ditunjukkan pada gambar 5.

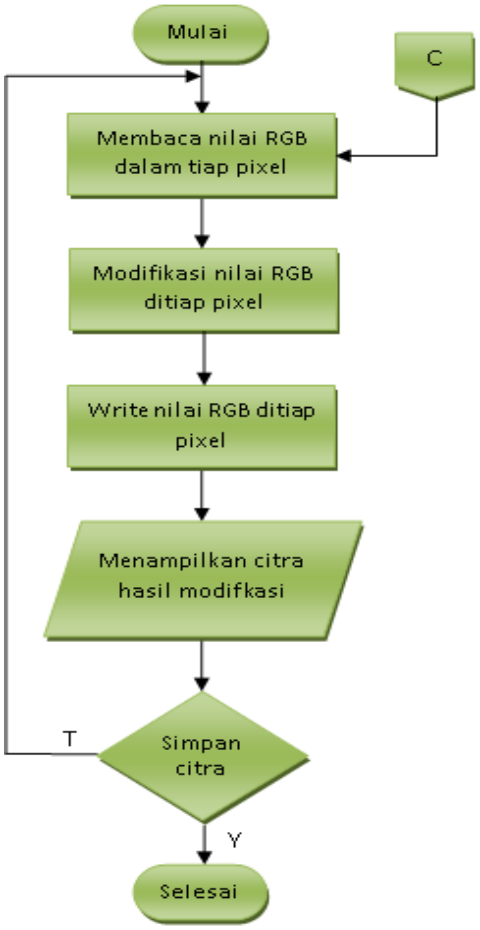
ISSN : 2723 - 4193
E-ISSN : 2775-8338



Gambar 5. Diagram alir proses penyisipan citra pesan

Diagram alir pada Gambar 5 memperlihatkan proses penyisipan citra pesan menggunakan fungsi hash (MD5) dan algoritma DES. Proses ini yang pertama dilakukan adalah mengambil nilai dari komponen warna citra penampung dalam tiap-tiap pixel dan mengubahnya ke nilai hexadesimal, kemudian diubah dalam bentuk biner. Sebagai contoh, jika ada suatu komponen warna bernilai 164 diubah menjadi A4 dalam bentuk hexadesimal, kemudian diubah ke bentuk biner menjadi 10100100. Sementara itu citra pesan yang akan disisipkan diproses terlebih dahulu menggunakan fungsi hash (MD5). Pesan dibagi menjadi *L* buah blok yang masing-masing panjangnya 512 bit. Setiap blok 512 bit diproses bersama dengan penyangga MD menjadi keluaran 128 bit. Output proses fungsi hash (MD5) kemudian masuk ke proses enkripsi DES. Blok data yang berukuran 128 bit dibagi menjadi dua bagian yaitu 64 bit *plaintext* dan 64 bit kunci. Blok pesan inilah yang diolah dalam proses enkripsi DES seperti yang telah dijelaskan pada sub bab 2.3. Kemudian bit pertama *ciphertext* yang ingin disisipkan kedalam berkas bitmap dimasukkan dalam komponen warna merah, bit berikutnya dalam komponen warna hijau, bit berikutnya lagi dalam komponen warna biru pada pixel pertama. Satu bit *ciphertext* berikutnya dimasukkan dalam komponen warna merah, bit berikutnya lagi dimasukkan pada komponen warna hijau, bit berikutnya lagi dimasukkan pada komponen warna biru pada pixel kedua. Begitu seterusnya sampai *ciphertext* bit yang terakhir. Setelah selesai proses penyisipan maka selanjutnya adalah menampilkan citra hasil pada *form*.

Bagian keempat adalah diagram alir untuk proses modifikasi citra hasil steganografi. Diagram alir dari proses modifkasi ditunjukkan pada Gambar 6.



Gambar 6. Diagram alir proses modifikasi

ISSN : 2723 - 4193
E-ISSN : 2775-8338

3. Hasil Dan Pembahasan

Pada bagian ini akan dijelaskan mengenai hasil pengujian proses steganografi citra digital yang dimofikasi. Citra pesan yang digunakan berupa citra digital *.bmp. Parameter yang digunakan dalam pengujian ditampilkan dalam Tabel 2

Tabel 2 Parameter yang Digunakan dalam pengujian

Citra Penampung	Ukuran	Citra Pesan	Ukuran
Monalisa.bmp (783 x 1050) pixel	2,35 MB	Banana.bmp (292 x 287) pixel	245 KB
		Treasuremap .bmp (300 x 222) pixel	195 KB
		Twins.bmp (179 x 214) pixel	112 KB

3.1. Analisa Penyisipan Citra Pesan pada Citra Penampung

Pengujian dilakukan dengan menyisipkan tiga citra pesan yang memiliki ukuran berbeda-beda untuk melihat pengaruh proses penyisipan pesan terhadap perubahan nilai pixel, histogram serta nilai MSE dan PSNR.

Berdasarkan penelitian yang dilakukan, diperoleh data-data hasil penelitian yang ditunjukkan pada Gambar 7. Gambar 7(a) menunjukan citra penampung sebelum proses steganografi dilakukan. Gambar 7(b), Gambar 7(c), dan Gambar 7(d) berturut-turut menunjukan citra hasil steganografi yang telah mengandung citra pesan Banana.bmp, Treasuremap.bmp, dan Twins.bmp.

(a) (b) (c) (d)

Gambar 7. Perbandingan Pengaruh Penyisipan Citra Pesan Terhadap Citra Penampung

Berdasarkan pengamatan visual pada serangkaian citra pada Gambar 7, tidak terjadi perubahan yang signifikan terhadap citra penampung yang telah disisipkan citra pesan. Oleh karena itu, untuk melihat perubahan yang terjadi perlu ditinjau dari histogram, perubahan nilai pixel, serta nilai MSE dan PSNR.

4. Kesimpulan

Dari hasil analisis penggunaan steganografi dengan algoritma DES dan fungsi hash untuk mengatasi modifikasi citra, dengan menggunakan citra Banana.bmp, Treasuremap.bmp, dan Twins.bmp sebagai citra pesan, serta citra Monalisa.bmp sebagai citra penampung, maka dapat diambil kesimpulan bahwa:

1. Implementasi Algoritma DES dan Fungsi Hash pada teknik steganografi menghasilkan citra steganografi yang memiliki *robustness* terhadap modifikasi citra yang diujikan antara lain *fog, invert, mirror, lighten, darken*.
2. Semakin kecil ukuran citra pesan yang disisipkan maka semakin baik citra staganografi yang dihasilkan. Banana.bmp dengan ukuran 245 KB memiliki MSE sebesar 1,263E-03 dan PSNR sebesar 38,559 dB. Treasuremap.bmp dengan ukuran 195 KB memiliki MSE sebesar 8,957E-04 dan PSNR sebesar 39,305 dB. Twins.bmp dengan ukuran 195 KB memiliki MSE sebesar 2,809E-04 dan PSNR sebesar 41,822 dB.
3. Ukuran citra pesan tidak mempengaruhi besarnya *error* yang terjadi pada hasil dekripsi citra steganografi yang telah dimodifikasi. Contohnya pada modifikasi *invert*, Banana.bmp hasil dekripsi dengan ukuran 245 KB memiliki MSE sebesar 5,226E-03 dan PSNR sebesar 35,475 dB. Treasuremap.bmp dengan ukuran 195 KB memiliki MSE sebesar 1,725E-04 dan PSNR sebesar 42,882 dB. Twins.bmp dengan ukuran 195 KB memiliki MSE sebesar 6,395E-04 dan PSNR sebesar 40,036 dB.
4. Untuk jenis modifikasi yang tidak memerlukan nilai pengubah, *mirror horizontal* paling mempengaruhi citra pesan hasil dekripsi dengan nilai MSE dan PSNR masing-masing citra pesan yaitu 0,823 dan 24,488 dB untuk Banana.bmp, 0,525 dan 25,463 dB untuk Treasuremap.bmp, 0,589 dan 25,215 dB

ISSN : 2723 - 4193
E-ISSN : 2775-8338

untuk Twins.bmp. Sedangkan modifikasi yang memiliki sedikit pengaruh terhadap citra pesan hasil dekripsi adalah *invert* dan *mirror vertical* dengan nilai MSE dan PSNR masing-masing citra pesan yaitu 5,226E-03 dan 35,475 dB untuk Banana.bmp, 1,725E-04 dan 42,882 dB untuk Treasure.bmp, 6,395E-04 dan 40,036 dB untuk Twins.bmp.

Untuk jenis modifikasi yang memerlukan nilai pengubah, modifikasi *fog* (nilai pengubah 9 sebagai standar perbandingan) paling mempengaruhi citra pesan hasil dekripsi. Nilai MSE dan PSNR masing-masing citra pesan yaitu 1,273 dan 23,542 dB untuk Banana.bmp, 0,190 dan 27,668 dB untuk Treasuremap.bmp, 0,735 dan 24,735 dB untuk Twins.bmp. Sedangkan modifikasi yang memiliki sedikit pengaruh terhadap citra pesan hasil dekripsi adalah *darken* dengan nilai MSE dan PSNR masing-masing citra pesan yaitu 4,119E-04 dan 40,991 dB untuk Banana.bmp, 1,724E-04 dan 42,881 dB untuk Treasuremap.bmp, 6,394E-04 dan 40,036 dB untuk Twins.bmp.

5. Referensi

[1] Y. Septiani Muzahardin and A. Fauzi, "Perbaikan Citra Digital Pada Foto Dengan Menggunakan Metode Retinex," *J. Tek. Inform. Kaputama*, vol. 6, no. 1, pp. 133–139, 2022.

[2] Supiyandi Supiyandi, Muhammad Abdul Mujib, Khairul Azis, Rahmat Abdillah, and Salsa Nabila Iskandar, "Penerapan Teknologi Pengolahan Citra dalam Analisis Data Visual pada Tinjauan Komprehensif," *J. Kendali Tek. dan Sains*, vol. 2, no. 3, pp. 179–187, 2024, doi: 10.59581/jkts-widyakarya.v2i3.3796.

[3] A. R. Putri, "Pengolahan Citra Dengan Menggunakan Web Cam Pada Kendaraan Bergerak Di Jalan Raya," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 1, no. 01, pp. 1–6, 2016, doi: 10.29100/jipi.v1i01.18.

[4] I. P. Sari, F. Ramadhani, A. Satria, and D. Apdilah, "Implementasi Pengolahan Citra Digital dalam Pengenalan Wajah menggunakan Algoritma PCA dan Viola Jones," *Hello World J. Ilmu Komput.*, vol. 2, no. 3, pp. 146–157, 2023, doi: 10.56211/helloworld.v2i3.346.

[5] S. Mustafa, U. Muhammad, T. Elektro, P. Bosowa, T. Elektro, and P. Bosowa, "Rancang Bangun Sistem Monitoring Penggunaan Daya Listrik BERBASIS SMARTPHONE," *Jurbal Media Elektr.*, vol. 17, no. 3, pp. 127–130, 2020.

[6] W. S. Negoro, "Edukasi Pengolahan Citra Digital Untuk Pendeteksian Dan Informasi Pengetahuan Yang Tersembunyi Pada Citra Digital Image Processing Education for Detection and Knowledge Information Hidden in Images Abstrak," 2023.

[7] S. Mustafa, S. Nurfitri, A. J. Jauhar, R. Fuadi, and A. Rizal, "Rancang Bangun Media Pembelajaran Trainer PLC," *Joule (Journal Electr. Eng.*, vol. 3, no. 2, pp. 186–191, 2022, doi: 10.61141/joule.v3i2.324.

[8] J. Jumadi, Y. Yupianti, and D. Sartika, "Pengolahan Citra Digital Untuk Identifikasi Objek Menggunakan Metode Hierarchical Agglomerative Clustering," *JST (Jurnal Sains dan Teknol.*, vol. 10, no. 2, pp. 148–156, 2021, doi: 10.23887/jstundiksha.v10i2.33636.

[9] A. Ridhoi, "Penerapan Pengolahan Citra Untuk Perbaikan Gambar 2 Dimensi Dengan Menggunakan Matlab," *Joutica*, vol. 8, no. 1, pp. 64–69, 2023, doi: 10.30736/informatika.v8i1.1063.