KINERJA STEGANOGRAFI METODE *END OF FILE* PADA DATA CITRA DIGITAL

Lulu Maftukhatul Jannah[*)], Imam Santoso, dan Yuli Cristyono

Departemen Teknik Elektro, Universitas Diponegoro
Jl. Prof. Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)]*E-mail: lulu.mj016@gmail.com*

Abstrak

Steganografi merupakan teknik yang digunakan utuk menyembunyikan data ke dalam data lainnya. Pada Penelitian ini data yang disembunyikan atau disisipkan yaitu berupa pesan teks dan media penampung yang digunakan yaitu citra digital biner dan citra digital greyscale. Salah satu metode pada steganografi yaitu End of File. Pada Penelitian ini dirancang suatu sistem penyisipan data yang mana data akan disisipkan pada baris terakhir media penampung. Tujuan pembuatan Penelitian ini guna mendapatkan hasil citra stego yang baik yang dapat ditunjukkan dengan nilai PSNR. Nilai PSNR yang dihasilkan pada citra stego biner dan greyscale yaitu 100% diatas 20 dB. Berdasarkan hasil pengujian steganografi dengan variasi ukuran citra 592x525, 200x196 dan 75x98 yang akan disisipkan pesan dengan variasi panjang pesan sebanyak 7 karakter, 195 karakter dan 524 karakter, hasil dari penyisipan pesan kedalam citra akan menghasilkan empat format citra yaitu BMP, JPEG, PNG dan TIFF. Hasil desteganografi menunjukkan bahwa ketika pengungkapan pesan dilakukan tanpa adanya manipulasi citra, tingkat keberhasilan mencapai 75% .

Kata Kunci : steganografi, end of file, citra digital, PSNR

Abstract

Steganography is a technique used to hide data into the container media. In this Final Project the data is hidden or inserted in the form of text messages and media container used is a binary digital image and greyscale digital image. One method of steganography is End of File. In this Final Project designed a system of data insertion in which the data will be inserted in the last line of the container data. The purpose of this Final Project in order to get good stego image results that can be shown by the value of PSNR. The resulting PSNR value in the greyscale stego image is 100% above 20 dB and in the 75% stego binary image above 12 dB. Based on the results of steganography testing with image size variation of 592x525, 200x196 and 75x98 which will be inserted message with 7 characters character variation, 195 characters and 524 characters, the result of message insertion into image will produce four image format that is BMP, JPEG, PNG and TIFF. The results of desteganografi indicate that when the disclosure of the message done without image manipulation, the success rate reached 75%.

Keywords : steganography, end of file, digital image, PSNR

1. Pendahuluan

Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimiliki oleh internet maka internet untuk saat ini sudah menjadi hal yang tidak asing lagi. Sayangnya dengan berkembangnya internet dan aplikasi menggunakan internet semakin berkembang pula kejahatan sistem informasi. Dengan berbagai teknik, banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan perkembangan perkembangannya media internet ini harus juga dibarengi dengan pengamanan sistem informasi[1]. Namun sistem tersebut masih memerlukan metode tambahan agar tingkat akurasi dari suatu proses pengenalan bertambah, salah satunya dengan teknik steganografi. Steganografi dapat diartikan sebagai suatu teknik penyisipan atau penyembunyian informasi yang bersifat rahasia pada suatu data lainnya untuk sebagai "wadah", dimana orang lain tidak akan menyadari akan adanya data yang terkandung pada wadah tersebut. Penilaian sebuah algoritma steganografi yang baik dinilai dari beberapa faktor diantaranya keberadaan pesan rahasia dalam media penampung tidak dapat dipersepsi oleh indera manusia, kualitas atau mutu media penampung tidak berubah banyak akibat penyisipan, jumlah atau kapasitas informasi yang dapat disisipkan dan tahan terhadap berbagai operasi manipulasi media penampung serta pesan yang disembunyikan harus dapat diungkapkan kembali[2]. Beberapa penelitian dan pengembangan mengenai steganografi yang bertujuan untuk menyisipkan pesan kedalam citra telah dilakukan, beberapa diantaranya

menggunakan metode LSB (*List Significant Bit*) pada data *file* MP3[3] , DCT (*Discrete Cosine Transform*) pada data video[4], *Bit Plane Complexity Segmentation* pada data citra digital[5] dan *Spread Spectrum* pada data terkompresi JPEG[6].
Pada Penelitian ini akan membagahs tentang kinerja steganografi menggunakan metode *End of File* pada data citra digital. Berkas yang disisipkan yaitu berupa pesan teks, dan media penampungnya yaitu citra digital. Tingkat kualitas dari steganografi dalam Penelitian ini akan ditentukan berdasarkan nilai PSNR (*Peak Signal to Noise Ratio*) dan MSE (*Mean Square Error*).

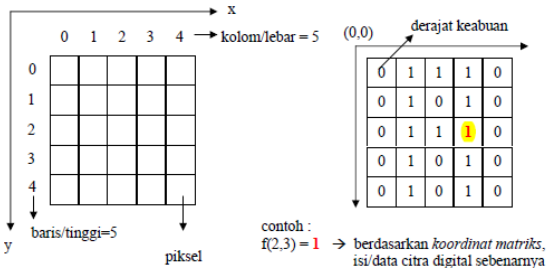
2. Metode

2.1. Steganografi

Steganografi adalah teknik menyembunyikan data rahasia di dalam media digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain. Steganografi membutuhkan dua bagian yang sangat penting yaitu berkas atau media penampung dan data rahasia yang akan disembunyikan. Penggunaan steganografi adalah untuk menyamarkan keberadaan data rahasia sehingga sulit di deteksi, dan juga dapat melindungi hak cipta dari suatu produk[7]. Kata steganografi berasal dari bahasa Yunani *steganos*, yang artinya tersembunyi atau terselubung, dan *graphein* artinya menulis. Kini, istilah steganografi termasuk penyembunyian data digital dalam file-file komputer[8].
Citra digital merupakan suatu matriks dimana indeks baris dan kolomnya menyatakan suatu titik pada citra tersebut dan elemen matriksnya (yang disebut sebagai elemen gambar/piksel/*piksel*/*picture element*/*pels*) menyatakan tingkat keabuan pada titik tersebut. Citra digital dinyatakan dengan matriks berukuran NxM (baris/tinggi = N, kolom/lebar = M)[12].

N = jumlah baris $0 \le y \le N-1$
M = jumlah kolom $0 \le x \le M-1$
L = maksimal warna intensitas $0 \le f(x,y) \le L-1$
(derajat keabuan / gray level)

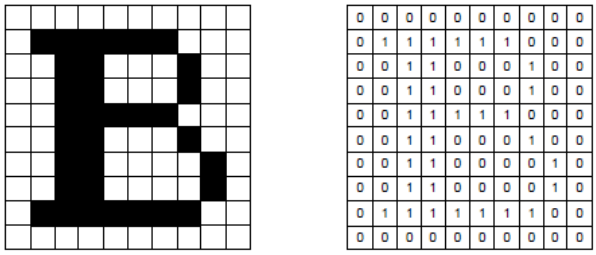
$$f(x,y)\begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & f(1,1) & \dots & f(1,(M-1) \\ : & : & : & : \\ f(N-1,0) & f(N-1,1) & \dots f(N-1,M-1) \end{bmatrix}$$



Gambar 1. Matriks citra digital[13]

Pada Penelitian ini akan membahas dua jenis yaitu citra biner dan citra *greyscale*. Berikut merupakan penjelasan dari citra biner dan citra *greyscale*.

Citra biner (*binary image*) adalah citra yang hanya mempunyai dua nilai derajat keabuan: hitam dan putih. Meskipun saat ini citra berwarna lebih disukai karena memberi kesan yang lebih kaya daripada citra biner, namun tidak membuat citra biner mati. Pada beberapa aplikasi citra biner masih tetap dibutuhkan, misalnya citra logo instansi (yang hanya terdiri atas warna hitam dan putih), citra kode batang (*bar code*) yang tertera pada label barang, citra hasil pemindaian dokumen teks, dan sebagainya. Gambar 2 merupakan tampilan dari citra biner dan representasinya.



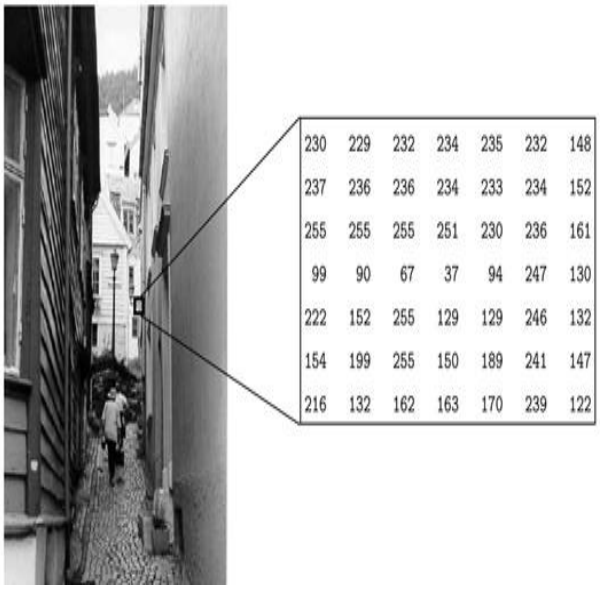
Gambar 2. Huruf "B" dan representasi biner

Berdasarkan Gambar 2 piksel-piksel objek bernilai 1 dan piksel-piksel latar belakang bernilai 0. Pada waktu menampilkan gambar, 0 adalah putih dan 1 adalah hitam. Jadi, pada citra biner, latar belakang berwarna putih sedangkan objek berwarna hitam. Alasan penggunaan citra biner adalah karena ia memiliki sejumlah keuntungan sebagai berikut:

1. Kebutuhan memori kecil karena nilai biner hanya membutuhkan representasi 1 bit. Kebutuhan memori untuk citra biner masih dapat berkurang secara berarti dengan metode pemampatan *run-length encoding* (*RLE*).
2. Waktu pemrosesan lebih cepat dibandingkan dengan citra *greys cale* karena banyak operasi pada citra biner yang dilakukan sebagai operasi logika (*AND*, *OR*, *NOT*, dll) ketimbang operasi aritmetika bilangan bulat. Aplikasi yang menggunakan citra biner sebagai masukan untuk pemrosesan pengenalan objek, misalnya pengenalan karakter secara optik, analisis kromosom, pengenalan *sparepart* komponen industri, dan sebagainya[11].

Citra *greyscale* merupakan citra digital yang hanya memiliki satu nilai kanal pada setiap pikselnya, dengan kata lain nilai bagian RED = GREEN = BLUE. Nilai tersebut digunakan untuk menunjukkan tingkat intensitas. Warna yang dimiliki adalah warna hitam, keabuan, dan putih. Tingkatan keabuan disini merupakan warna abu dengan berbagai tingkatan dari hitam hinnga mendekati putih[15]. Citra yang ditampilkan dari citra jenis ini terdiri atas warna abu-abu, bervariasi pada warna hitam pada

bagian yang intensitas terlemah dan warna putih pada intensitas terkuat. Citra *greyscale* berbeda dengan citra ”hitam-putih”, dimana pada konteks komputer, citra hitam putih hanya terdiri atas 2 warna saja yaitu ”hitam” dan ”putih” saja. Pada citra *greyscale* warna bervariasi antara hitam dan putih, tetapi variasi warna diantaranya sangat banyak. Citra *greyscale* disimpan dalam format 8 bit untuk setiap sample piksel, yang memungkinkan sebanyak 256 intensitas[16]. Gambar 3 merupakan citra *greyscale* dan representasi nilai *piksel*nya.



Gambar 3. Citra *greyscale* dan representasi *piksel* [17]

2.2. End Of File

End of file (EoF) adalah salah satu algoritma yang dapat digunakan dalam steganografi, algoritma ini melakukan penyisipan pesan dengan teknik pesan akan disisipkan pada akhir file media penampung. Metode EoF dikenal sebagai algoritma injeksi, teknik ini secara langsung menambahkan pesan pada akhir *file*. Keberhasilan algoritma injeksi menyisipkan pesan pada media penampung akan mempertahankan kualiatas media penampung. Tetapi metode ini secara signifikan akan mempengaruhi ukuran *file stego*[20], karena penyisipan pesan diletakkan di akhir berkas. Sebelum disisipkan, pesan diubah terlebih dahulu berdasarkan citra yang digunakan, jika yang digunakan citra biner maka pesan akan diubah menjadi bir biner, jika yang digunakan citra *greyscale* maka pesan akan diubah menjadi kode ASCII. Misalnya pada sebuah citra *greyscale* skala keabuan 6x6 piksel disisipkan pesan yang berbunyi “#aku”.
Kode ASCII dari pesan adalah:

35 97 107 117
a k u

Misalkan matriks tingkat derajat keabuan citra sebagai berikut.

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	125	190	190	200

Kolom citra yang akan disisipi

Kode ASCII pesan disisipkan diakhir citra, sehingga citra menjadi[15]:

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	125	190	190	200
35	97	107	117		

Kode ASCII pesan

2.3. Kinerja Steganografi

Pengembang dan pelaksana metode kompresi citra berugi membutuhkan standar pengujian untuk mengukur kualitas dari citra yang telah dimodifikasi (diberi *noise* atau diberikan efek khusus) dengan citra asli. Citra yang sudah dimodifikasi lebih baik menyerupai citra yang asli, agar kualitas citra teteap terjaga. Kualitas citra yang diukur biasanya berdasarkan perhitungan *peak signal to noise ratio* (PSNR). Semakin besar PSNR nilai berarti citra yang dimodifikasi mirip dengan citra asli[22].

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya noise yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan desibel. Pada penelitian kali ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai rata-rata kuadrat dari error (MSE-*Mean Square Error*)[15]. Perhitungan MSE adalah sebagai berikut:

$$\text{MSE} = \frac{1}{mn}\sum_{i}^{m}\sum_{j}^{n} \| I(i,j) - K(i,j) \|^2 \qquad (1)$$

dengan:
MSE = Nilai Mean Square Error dari citra tersebut
m = panjang citra tersebut (dalam piksel)
n = lebar citra tersebut (dalam piksel)
(i,j) = koordinat masing-masing piksel
I = nilai bit citra pada koordinat i,j
K = nilai derajat keabuan citra pada koordinat i,j

MSE merupakan rata-rata kuadrat dari eror (perbedaan piksel citra) dari citra yang telah dimodifikasi dengan citra

asli. Root mean square error (RMSE) didefinisikan sebagai akar kuadrat dari MSE[19]. Sementara nilai PSNR dihitung dari kuadrat nilai maksimum sinyal dibagi dengan MSE. Apabila diinginkan PSNR dalam desibel, maka nilai PSNR akan menjadi sebagai berikut[15]:

$$\text{PSNR}=20.log_{10}\left(\frac{MAX_i}{\sqrt{MSE}}\right) \quad (2)$$

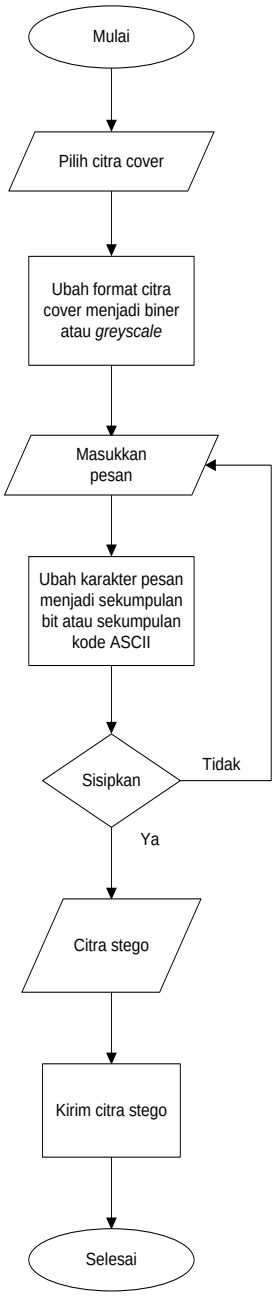
dengan:
PSNR = nilai PSNR citra (dalam dB)
MAXi = nilai maksimum piksel
MSE = nilai MSE

Untuk citra biner nilai pembilang adalah 1. Untuk citra *greyscale* yang mempunyai bobot 8 bit per piksel, pembilangnya adalah 255. Semakin besar kemiripan antara citra yang dimodifikasi dengan citra asli maka nilai RMSE akan semakin kecil, dengan kata lain nilai PSNR akan semakin besar. PSNR tidak mempunyai dimensi, karena kedua pembilang dan penyebut merupakan nilai piksel, meskipun demkian berdasarkan persamaan 2.2 PSNR diekspresikan dalam *decible* (dB).

2.4. Perancangan

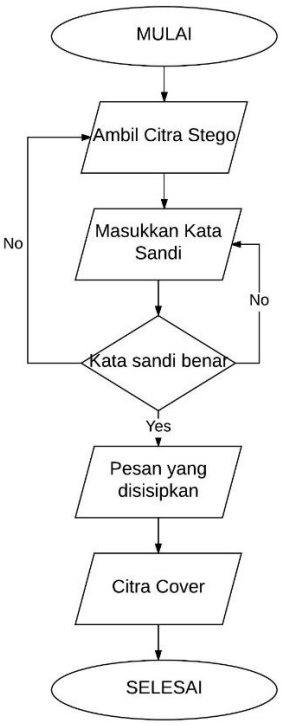
Pada Penelitian ini terdiri dari dua proses, yang pertama adalah tahap steganografi dan desteganografi. Tahap steganografi merupakan tahap dimana dilakukannya penyisipan karakter pesan kedalam citra *cover*. Langkah awal pada tahap ini adalah memilih citra yang akan digunakan sebagai citra *cover*. Citra yang dipilih akan merupakan citra RGB yang mana dalam citra tersebut akan diubah menjadi citra biner atau citra *greyscale*. Citra *cover* yang sudah diubah menjadi biner atau *greyscale* berarti sudah siap untuk disisipkan oleh karakter pesan. Pesan yang disisipkan mempunyai *limit* atau batas yaitu sama dengan panjang dari ukuran citra *cover*. Karakter pesan yang akan disisipkan kedalam citra harus sudah dalam bentuk sekumpulan bit atau sekumpulan kode ASCII. Sekumpulan bit atau sekumpulan kode ASCII tersebut yang akan disisipkan kedalam citra, dimana letak dari sekumpulan bit dan kode ASCII tersebut akan ditempatkan pada akhir baris citra *cover,* hal tersebut menyebabkan ukuran citra *cover* bertambah. Setelah penyisipan selesai dilakukan maka citra stego akan dikirimkan kepada penerima, yang mana pada sisi penerima akan dilakukan proses desteganografi, yang mana pada proses ini akan dilakukan pengungkapan pesan yang telah disisipkan sebelumnya.

Diagram alir proses steganografi ditampilkan oleh Gambar 4.



Gambar 4. Diagram alir proses steganografi

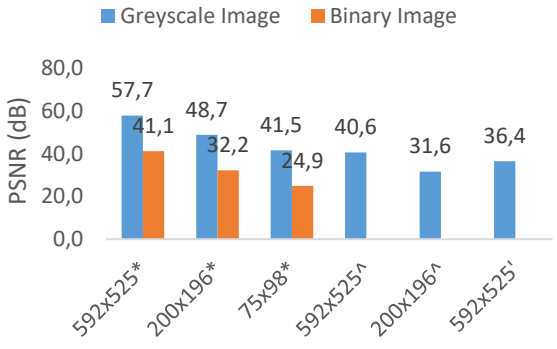
Proses yang kedua adalah proses desteganografi merupakan tahap diungkapkannya kembali pesan yang telah disisipkan, sehingga penerima dapat memahami pesan yang terkandung didalam citra stego. Pada tahap desteganografi ini terdapat proses manipulasi citra yang mana citra stego akan diberikan noise (*blurring* dan *salt and pepper*), diubah letak pikselnya (*rotation* 90^0), dan diperbaiki kualitasnya (*sharpen*). Tujuan dilakukkan tahap edit citra adalah untuk meneliti dan menganalisa ketahanan citra stego jika diberikan efek tertentu, apakah pesan yang disisipkan tetap utuh atau akan rusak dan tidak dapat dipahami. Diagram alir proses desteganografi ditampilkan oleh Gambar 5.



Gambar 5. Diagram alir proses desteganografi

3. Hasil dan Analisa

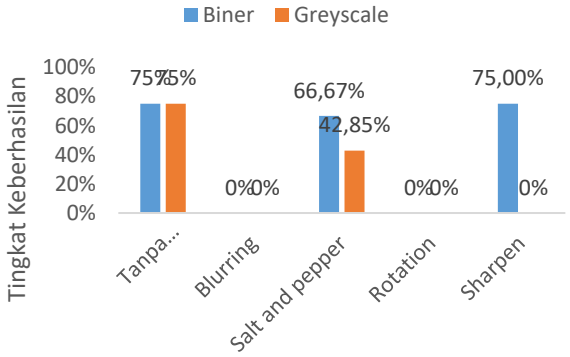
Pengujian PSNR dengan variasi jumlah karakter pesan yang berbeda yaitu 7 karakter, 196 karakter dan 525 karakter, ukuran yang berbeda yaitu 593x525, 201x196 dan 76x98, dan format citra yang bebeda yaitu BMP, JPEG, PNG dan TIFF. Nilia PSNR menunjukkan kualitas citra stego berdasarkan perbandingan antara citra *cover* (citra asli) dan citra stego (citra sisipan). Berdasarkan grafik pada Gambar 6 dapat disimpulkan nilai PSNR yang baik terdapat pada format citra BMP , nilai PSNR bergantung pada ukuran citra dan jumlah karakter pesan yang dimasukkan. Gambar 6 menunjukkan perbandingan nilai PSNR yang didapat.



Gambar 6. Grafik perbandingan nilai PSNR yang diperoleh

Pada Gambar 6 dapat dilihat bahwasanya terdapat karakter "*" yang menunjukkan masukkan pesan berjumlah 7 karakter, karakter "^" menunjukkan masukkan pesan berjumlah 196 karakter, dan karakter " ' " menunjukkan masukkan pesan berjumlah 525 karakter. Berdasarkan nilai PSNR yang diperoleh dapat disimpulkan bahwa terdapat hubungan antara jumlah karakter dan ukuran citra stego, semakin banyak karakter yang disisipkan pada citra stego dengan ukuran a, b atau c maka nilai PSNR semakin kecil.

Pengujian dengan hasil desteganografi. Hasil desteganografi pada Penelitian dibedakan menjadi dua bagian yaitu tanpa manipulasi citra stego dan dengan manipulasi citra stego. Manipulasi citra stego yang dilakukan adalah dengan memberikan *noise blurring* dan *salt and pepper*, perubahan letak nilai piksel (*rotation* 90^0) dan penajaman (*sharpen*).



Gambar 7. Grafik Akurasi hasil desteganografi pada citra stego

Pada Gambar 7 dapat dilihat secara keseluruhan bahwa akurasi tertinggi dicapai pada saat citra stego tidak diberikan manipulasi apapun, hal tersebut dikarenakan nilai piksel tidak berubah, sedangkan untuk citra stego yang diberikan manipulasi nilai piksel citra berubah karena efek dari pemberian manipulasi tersebut. Jika diamati secara rinci hasil tertinggi desteganografi dengan manipulasi citra terdapat pada citra stego biner dengan manipulasi penajaman citra (*sharpen)*. Hasil destegano dengan manipulasi *blurring* keadaan pesan telah rusak dan tidak dapat dipahami, dan dengan manipuasi *rotation* pesan tidak dapat ditampilkan karena saat proses destegano dilakukan nilai piksel pada baris terakhir yang akan diubah karakternya tidak terdapat informasi (pesan) didalamnya.

4. Kesimpulan

Berdasarkan hasil pengujian yang dilakukan, diperoleh beberapa point yang perlu diperhatikan sebagai berikut. Pada citra biner sebanyak 95.4% menyatakan tidak ada perbedaan antara citra asli dan citra stego, dan pada citra greyscale sebanyak 80.7% menyatakan tidak ada perbedaan antara citra asli dan citra stego. Hal tersebut membuktikan bahwa kriteria imperceptibility sudah

tercapai. Pada citra greyscale PSNR terbesar mencapai 57.7 dB dan PSNR terendah yaitu mencapai 35.4 dB. Pada citra biner nilai PSNR terbesar yang didapatkan yaitu sebesar 41.1 dan nilai PSNR terendah yaitu sebesar 24.9 dB. Hal tersebut membuktikan bahwa kriteria fidelity sudah tercapai. Hasil desteganografi tanpa diberikan manipulasi pada citra stego pada format citra BMP, PNG dan TIFF, tingkat keberhasilannya mencapai 100%. Hal tersebut membuktikan bahwa kriteria recovery sudah tercapai.Hasil desteganografi tanpa diberikan manipulasi pada citra stego pada format JPEG tingkat keberhasilannya mencapai 0%. Hal tersebut membuktikan bahwa kriteria recovery tidak tercapai. Tingkat keberhasilan desteganografi setelah diberi manipulasi pada citra stego biner dan greyscale dengan manipulasi blurring, rotasi dan salt and pepper kriteria recovery belum tercapai, sedangkan pada citra stego biner dengan manipulasi sharpen kriteria recovery sudah tercapai. Pada citra biner dan greyscale citra stego format BMP, PNG dan TIFF (tanpa diberikan manipulasi) sudah dapat dikatakan baik karena sudah memenuhi kriteria steganografi. Citra biner dan greyscale yang diberikan manipulasi belum dapat dikatakan baik karena tidak memenuhi kriteria steganografi.

Referensi

[1]. F. Surur, M. Abdurohman, and E. M. Dharma, "Peningkatan Ketahanan Steganografi *Low Bit Code* Pada *File* Mp3 Dengan Pengurangan Distorsi LSB (*Least Significant Bit*) *Coding*," 2007.

[2]. P. Alatas, "Steganografi," *Implementasi Tek. Steganografi Dengan Metod. Lsb Pada Citra Digit.*, pp. 1–25, 2009.

[3]. D. E. Kurniawan and Narupi, "Teknik Penyembunyian Data Menggunakan Kombinasi Kriptografi Rijndael dan Steganografi Least Significant Bit (LSB)," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 3, pp. 254–262, 2016.

[4]. A. Y. Qadarisman, "Steganografi Video Dengan Menggunakan Metode Discrete Cosine Transform (Dct) Aditya Yuda Qadarisman," 2011.

[5]. A. Solichin and N. P. Wulandari, "Implementasi Steganografi Dengan Metode Bit Plane Complexity Segmentation Untuk Menyembunyikan," *SESINDO*, no. November, pp. 2–3, 2015.

[6]. W. Winanti, "Penyembunyian Pesan pada Citra Terkompresi JPEG Menggunakan Metode Spread Spectrum," *Communications*, no. 13505017, 2009.

[7]. Edisuryana Mukharrom, Isnanto R Riza, and Somantri Maman, "Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End of File," *Transien*, vol. 2, no. 3, pp. 1–9, 2013.

[8]. Y. Aditya, A. Pratama, and A. Nurlifa, "Studi pustaka untuk steganografi dengan beberapa metode," vol. 2010, no. Snati, pp. 32–35, 2010.

[9]. Krisnawati, "Metode Least Significant Bit (Lsb) Dan End of File (Eof)," *Seminar*, vol. 2008, no. semnasIF, pp. 39–44, 2008.

[10]. M. Irawan, "Penggunaan Steganografi dengan Metode End of File (EOF) pada Digital Watermarking," vol. 2, no. 1, pp. 36–42, 2013.

[11]. Munir, R., Pengolahan Citra Digital dengan Pendekatan Algoritmik, Informatika, Bandung, 2004.

[12]. D. YURISNA, "RANCANG BANGUN APLIKASI PENGECEKAN LEMBAR JAWABAN KOMPUTER (LJK) UNTUK TES PSIKOLOGI ROTHWELL MILLER INTEREST BLANK (RMIB) (Studi Kasus: CV. MatahariQu)," 2011.

[13]. M. Imron, "Pengolahan Citra," pp. 1–44, 2013.

[10]. P. Alatas, "Steganografi," *Implementasi Tek. Steganografi Dengan Metod. Lsb Pada Citra Digit.*, pp. 1–25, 2009.

[14]. Miftahur Rahim A. A, "TEKNIK PENYEMBUNYIAN DATA RAHASIA DENGAN MENGGUNAKAN CITRA DIGITAL SEBAGAI BERKAS PENAMPUNG," pp. 1–8.

[16]. H. Al Fatta, "Konversi Format Citra Rgb Ke Format Grayscale Menggunakan Visual Basic," vol. 2007, no. November, pp. 1–6, 2007.

[17]. D. I. Surya and Saputra, "Peningkatan Kualitas Citra," 2014.

[18]. E. Sujatmiko, R. R. Isnanto, and E. Handoyo, "Pemilihan Algoritma Optimal untuk Kompresi Data Citra Iris Mata Manusia."

[19]. H. Crisnanto, "PENGENDALIAN KUALITAS CAIRAN DALAM BOTOL BERBASIS PENGOLAHAN CITRA," 2011.

[20]. Hidayatno, A., Penapisan Citra – Pengolahan Citra Digital, Teknik Elektro, Universitas Diponegoro.

[21]. D. Ariyus, Pengantar IlmuKriptografi Teori, Analisis, dan Implementasi. Andi Offset, Yogyakarta. 2008.

[22]. D. Salomon, *Data Compression*. 2007.