Steganografi Pada Citra Menggunakan Histogram Shifting dan Difference Expansion

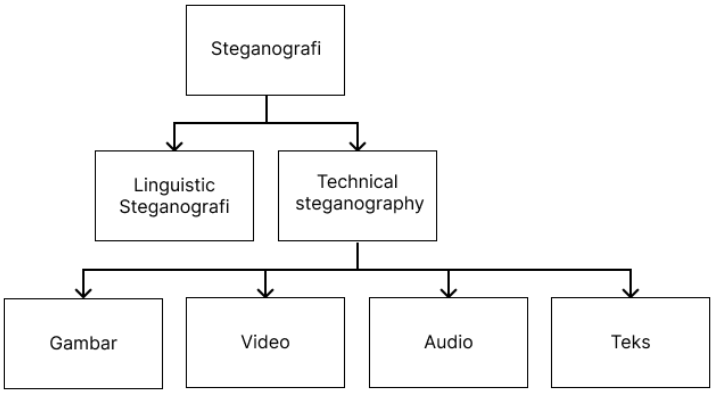
ABSTRAK

–Kerahasiaan informasi merupakan hal yang sangat dibutuhkan dalam menjaga keamanan penyebaran informasi dan steganografi merupakan salah satu metode untuk merahasiakan data. Masalah yang dihadapi dalam steganografi adalah adanya distorsi yang dapat terjadi pada citra saat pesan disembunyikan di dalamnya sehingga mengurangi tujuan dari steganografi yang mana menyisipkan pesan kedalam citra tanpa menyebabkan perubahan pada kualitas visual.. Hal ini membuat perlunya algoritma yang dapat melakukan proses penyisipan dengan efek distorsi seminimal mungkin. Histogram Shifting dan Difference Expansion digunakan sebagai metode dalam algoritma yang diusulkan. Keterbaruan dalam penelitian ini terletak pada penggunaan metode Histogram Shifting dan Difference Expansion yang dimodifikasi menjadi lebih sederhana. Selain itu, penelitian ini mengusulkan algoritma penyisipan yang inovatif. Citra stego dievaluasi menggunakan PSNR. Hasil pengujian menunjukkan jika alpha yang merupakan bagian dari proses perhitungan Histogram Shifting memiliki pengaruh yang signifikan terhadap kualitas citra. Serta pada pengujian kualitas citra stego dengan ukuran payload yang bervariasi menunjukkan jika algoritma yang diusulkan mampu mempertahankan kualitas citra dan menghasilkan skor PSNR rata-rata diatas 40dB

PENDAHULUAN

Keamanan informasi memiliki peran yang sangat penting dalam menjaga kerahasiaan informasi. Ada dua pendekatan umum untuk merahasiakan data yaitu kriptografi dan steganografi [1]. Konsep pada kriptografi adalah mengubah informasi tersebut menjadi tidak dapat dibaca dan dimengerti (Kumar, et al., 2021). Meskipun terdapat banyak metodologi yang tangguh dan sangat aman, perkembangan masih terus dilakukan untuk membuat teknik-teknik ini lebih aman dan tangguh dalam hal pengukuran kinerja [2]. Penyembunyian data menyembunyikan data rahasia dalam wadah media (dapat berupa gambar digital) sebagai metode yang telah diusulkan untuk melindungi keamanan [3]. Steganografi adalah salah satu metode yang digunakan untuk menyembunyikan data atau pesan rahasia ke dalam media yang tampak normal, seperti citra. Dengan menggunakan steganografi, informasi rahasia tersebut ditransfer dengan aman dengan menyematkan informasi ini di bawah penutup. Dengan demikian, data bergerak dalam penyamaran, tidak terdeteksi oleh penyadap [4].

Dalam steganografi, sering kali terjadi distorsi pada citra yang dapat mempengaruhi kejelasan visual dan kualitas citra secara keseluruhan. Demi alasan keamanan dan ketidakterlihatan, sangat penting bagi citra stego untuk tidak menunjukkan artefak atau distorsi yang terlihat. Citra asli dan citra stego harus terlihat persis sama dalam semua kemungkinan perbandingan [5]. Masalah utama yang ingin dipecahkan dalam penelitian ini adalah meminimalisasi distorsi yang mungkin terjadi pada citra akibat proses steganografi menggunakan algoritma yang diusulkan. Oleh karena itu, perlu dilakukan evaluasi untuk melihat sejauh mana teknik histogram shifting dan difference expansion dapat mempengaruhi kualitas citra.



Gambar 1. Klasifikasi penyembunyian data [6]

[7] memaparkan metode untuk penyisipan data yang dapat dipulihkan pada citra digital menggunakan teknik difference expansion. Teknik ini memanfaatkan kelebihan dalam citra digital untuk mencapai kapasitas penyisipan yang tinggi dan distorsi yang rendah. Metode ini melibatkan perhitungan perbedaan nilai pada piksel tetangga dan pemilihan beberapa nilai perbedaan untuk teknik difference expansion. Informasi untuk me-restorasi konten asli, kode autentikasi pesan, dan data tambahan semua disisipkan ke dalam nilai perbedaan tersebut. Metode ini menujukkan performa yang sangat baik dengan hasil pengujian rata-rata mendapat skor PSNR diatas 44dB.

Selanjutnya, Histogram Shifting pertama kali diperkenalkan oleh [8]. Metode ini berfokus pada penggunaan frekuensi piksel paling banyak dalam sebuah citra untuk proses penyisipan. Proses penyisipan melibatkan tiga langkah utama. Pertama menemukan nilai piksel dengan frekuensi terbanyak (peak) dan nilai piksel dengan frekuensi terendah (minimum). Setelah itu disediakan ruang untuk menyisipkan data dengan cara menggeser piksel diantara piksel peak dan piksel minimum. Metode ini mampu menyisipkan sekitar 5-80 Kb data kedalam citra grayscale berukuran 512x512 dengan skor PSNR yang didapat diatas 48dB.

Lalu pada riset [9] menyajikan gambaran umum tentang teknik histogram shifting sebagai metode penyembunyian data. Artikel tersebut membahas ide dasar dari histogram shifting, yang melibatkan penemuan titik nol dan titik puncak dalam histogram citra untuk meningkatkan kapasitas muatan. Artikel juga menggambarkan perkembangan terakhir dalam teknik ini, termasuk peningkatan kapasitas muatan dan kualitas citra. Para penulis memberikan tinjauan komprehensif terhadap literatur mengenai histogram shifting, termasuk berbagai metode dan aplikasinya. Artikel ini menyimpulkan bahwa histogram shifting adalah teknik yang menjanjikan untuk penyembunyian data dan memiliki potensi untuk pengembangan dan perbaikan lebih lanjut.

Pada penelitian [10] menjelaskan skema penyembunyian data yang dapat dipulihkan secara adaptif berdasarkan prediksi difference expansion. Skema yang diusulkan memanfaatkan kapasitas penyisipan dengan memanfaatkan sepenuhnya jumlah yang besar dari nilai perbedaan yang lebih kecil di mana data rahasia dapat disisipkan. Skema ini menawarkan beberapa keunggulan, yaitu peta lokasi tidak lagi diperlukan, kapasitas penyisipan dapat disesuaikan tergantung pada aplikasi praktis, dan kapasitas penyisipan yang tinggi dengan distorsi visual yang minimal dapat dicapai. Hasil-hasil eksperimen menunjukkan bahwa skema yang diusulkan menghasilkan kapasitas penyisipan yang tinggi dengan membandingkan skema terkait yang diusulkan baru-baru ini.

[11] mengusulkan metode data hiding untuk menyisipkan data rahasia pada piksel referensi menggunakan teknik difference expansion, histogram shifting, dan interpolation. Metode yang diusulkan memperbaiki metode sebelumnya dengan memungkinkan piksel referensi digunakan untuk menyisipkan data rahasia dan meningkatkan kapasitas penyembunyian. Metode ini melibatkan klasifikasi piksel, perhitungan piksel interpolasi, perhitungan perbedaan, dan penyisipan data. Ini bertujuan untuk meningkatkan kapasitas penyembunyian sambil menjaga kualitas citra dan keaman karena data rahasia dapat dienkripsi. Penelitian ini memberikan kesimpulan bahwa metode yang diusulkan berdasarkan difference expansion, histogram shifting, dan interpolation memberikan kapasitas penyembunyian data yang lebih tinggi.

Penelitian ini berfokus pada pengembangan algoritma dan meningkatkan kualitas citra stego dari metode terdahulu. Metode Histogram Shifting dan Difference Expansion akan diterapkan dengan memodifikasi metode tersebut. Pada algoritma yang diusulkan juga menggunakan teknik penyisipan pesan baru pada domain spasial.

METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian diawali dengan mengidentifikasi masalah yang ada. Lalu melakukan tinjauan pustaka dari penelitian terdahulu. Setelah itu masuk kedalam tahap pembuatan algoritma. Algoritma dibuat dengan dua metode, yaitu Histogram Shifting dan Difference Expansion. Kedua metode yang dipakai melalui proses modifikasi agar dapat menyesuaikan dengan kebutuhan penelitian. PSNR menjadi metriks utama yang digunakan pada pengujian untuk mengukur kualitas citra stego. Pengujian algorima dilakukan dengan dua tahap. Yaitu, pengujian variasi payload dan pengujian variasi alpha. Dalam pengujian dijabarkan hasil evaluasi dari citra stego menggunakan PSNR. Pengujian mencakup perbandingan skor PSNR antar citra stego dengan variasi alpha dan variasi payload yang berbeda-beda. Pengujian ini dilakukan untuk mengevaluasi sejauh mana algoritma steganografi yang diusulkan dapat mempertahankan kualitas citra.

2.2 Metodologi Penelitian

a. Histogram Shifting Method

Histogram Shifting pertama kali diperkenalkan oleh [8]. Skema Histogram-based terkenal karena kemudahannya dalam implementasi dan kebutuhan overhead yang rendah untuk proses dekoding [12]. Ide dari metode ini adalah menggunakan warna dengan frekuensi terbanyak dalam citra [13]. Pada dasarnya Histogram Shifting melibatkan perubahan nilai piksel dalam citra dengan cara menambahkan atau mengurani nilai tertentu. Tujuan dari pergeseran histogram adalah untuk menyembunyikan pesan rahasia dengan memanfaatkan karakteristik distribusi piksel pada citra. Metode Histogram Shifting yang diimplementasikan pada penelitian ini telah dimodifikasi secara khusus. Modifikasi dilakukan dengan tujuan untuk menyederhanakan metode dan meningkatkan efektivitas algoritma. Di mana persamaan modifikasi sebagai berikut:

$$l = m + alpha * n \quad (1)$$

Dimana l merupakan nilai piksel dihitung dengan menambahkan nilai alpha dikalikan dengan bit pesan rahasia (n) lalu ditambahkan dengan nilai piksel asli (m). Jika bit pesan rahasia yang akan disisipkan adalah 0 maka nilai piksel asli tidak akan berubah, dan sebaliknya jika bit pesan rahasia yang akan disisipkan adalah 1 maka nilai piksel akan berubah dipengaruhi oleh nilai alpha.

b. Difference Expansion Method

Metode ini melakukan perhitungan perbedaan nilai piksel yang berdekatan, kemudian memilih beberapa nilai perbedaan tersebut untuk dijadikan sebagai perluasan perbedaan [7]. Pada dasarnya, difference expansion melibatkan manipulasi nilai perbedaan antara piksel-piksel tetangga dalam citra. Nilai perbedaan ini dapat diubah dengan menambahkan atau mengurangi sejumlah nilai yang merepresentasikan pesan rahasia. Selama proses ini, perubahan nilai perbedaan yang terjadi haruslah kecil sehingga tidak mengakibatkan distorsi yang signifikan pada citra.

Pada implementasinya metode Difference Expansion juga mengalami perubahan. Konsep yang diaplikasikan mencakup persamaan yang dirancang untuk proses Difference Expansion yang lebih sederhana. Persamaan tersebut dijabarkan sebagai berikut:

$$l = l + diff \quad (2)$$

Dimana perbedaan tersebut adalah:

$$diff = l - m \quad (3)$$

nilai piksel (l) merupakan nilai piksel setelah proses Histogram Shifting. Sehingga dicari nilai diff terlebih dahulu, kemudian proses Difference Expansion berjalan setelahnya. Perbedaan didapatkan dari nilai piksel sesudah melewati proses histogram shifting dikurangi dengan nilai piksel asli pada citra.

c. Algoritma yang diusulkan

Ide dari proses penyisipan pada penelitian ini adalah dengan menyisipkan satu bit biner pesan rahasia kedalam tiap satu piksel secara berurutan dengan cara memodifikasi nilai piksel tersebut agar dapat menyimpan informasi nilai biner. Alur algoritma dapat dilihat pada gambar 2.

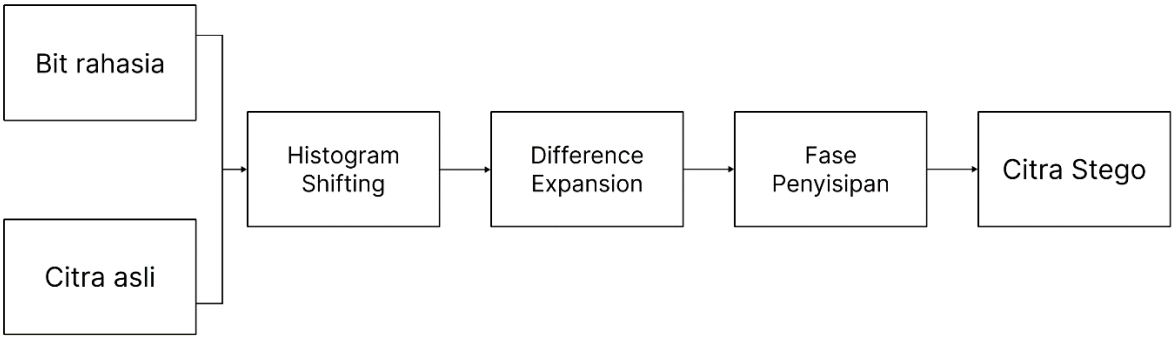
Langkah pertama dalam algoritma ini adalah mengubah citra asli menjadi citra grayscale. Lalu pesan rahasia yang ditulis dalam bentuk karakter diubah kedalam biner 8 bit. Kumpulan biner tersebut selanjutnya dibentuk kedalam

matriks dengan ukuran yang sama dengan citra asli, sehingga pada piksel dengan koordinat (x,y) akan disisipkan pesan dengan koordinat yang sama (x,y) dari matriks. Iterasi dilakukan pada setiap nilai piksel dan akan melalui proses Histogram Shifting dan Difference Expansion.

Pada tahap Histogram Shifting, operasi dilakukan dengan menghitung variabel yang disebut “shifted_pixel”. Rumus metode Histogram Shifting pada algoritma ini dapat dilihat pada pembahasan Histogram Shifting diatas. Nilai variabel ini diperoleh dengan menambahkan nilai piksel asli dengan variabel alpha yang dikalikan dengan bit pesan biner. Alpha merupakan parameter yang digunakan untuk mengontrol sejauh mana perubahan nilai piksel yang diinginkan pada citra. Sedangkan bit pesan binary adalah pesan rahasia yang sebelumnya berbentuk teks, lalu diubah bentuknya menjadi binary matriks yang memiliki ukuran panjang dan lebar yang sama dengan citra.

Selanjutnya pada tahap Difference Expansion melibatkan perhitungan perbedaan (difference) antara piksel yang telah dimodifikasi hasil dari Histogram Shifting dengan nilai piksel asli, perhitungan ini akan menghasilkan “diff”. Setelah “diff” didapat, nilai “shifted_pixel” akan ditambahkan dengan nilai “diff”.

Lalu pada langkah selanjutnya terdapat aspek penting dalam penyisipan pesan, yaitu pengaturan digit terakhir dari nilai piksel. Digit terakhir dimodifikasi agar sesuai dengan nilai biner pesan rahasia. Misalkan jika bit biner yang disisipkan 1, maka ubah digit terakhir nilai piksel ke angka tertentu. Dan juga sebaliknya jika biner pesan rahasia adalah 0. Angka tertentu ini akan disimpan dalam array yang disebut array kunci. Langkah ini akan dijelaskan lebih detail pada bagian penyisipan.

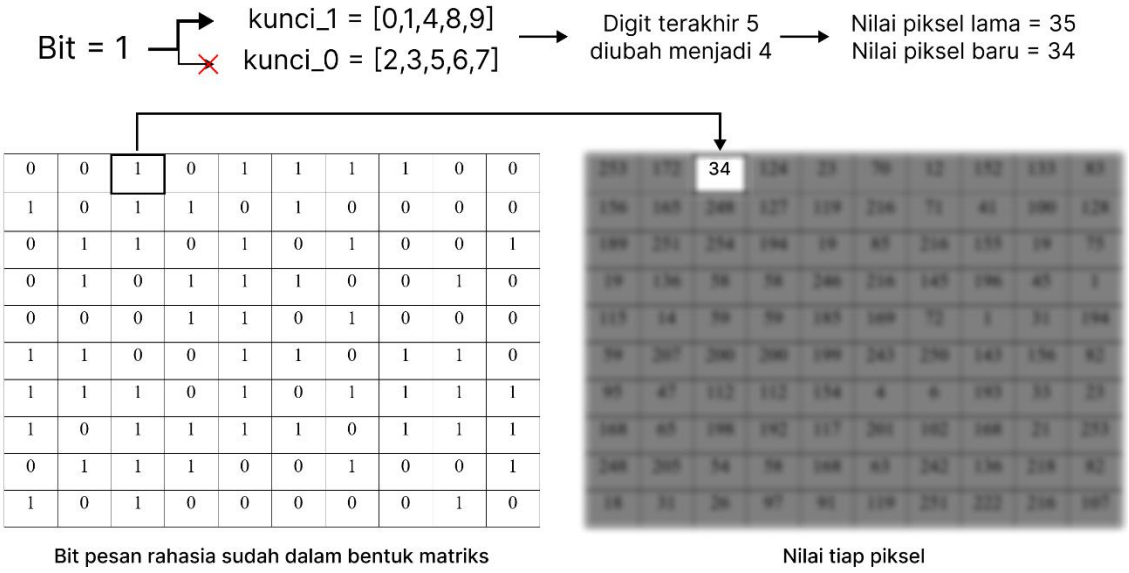


Gambar 2. Alur Algoritma

d. Fase Penyisipan

algoritma steganografi yang dibuat pada penelitian ini melakukan penyisipan pada domain spasial, proses ini menggunakan nilai piksel yang dimodifikasi untuk melakukan proses penyisipan. Pada dasarnya, nilai piksel diubah ke nilai tertentu untuk mengindikasikan bit pesan rahasia pada piksel tersebut. modifikasi nilai piksel dilakukan dengan menentukan digit terakhir dari nilai piksel mengacu kepada bit pesan rahasia yang akan disisipkan. Proses ini melibatkan dua kunci, satu kunci untuk biner pesan rahasia 0 dan satu lagi untuk biner pesan rahasia 1. Kunci ini berbentuk array berisi kumpulan angka yang dimaksudkan untuk menjadi pengganti nilai digit terakhir dari nilai piksel. Pada algoritma digunakan array kunci_1 = [0, 1, 4, 8, 9] dan kunci_0 = [2, 3, 5, 6, 7].

Cara kerjanya adalah jika biner pesan rahasia yang akan disisipkan adalah 1, maka digit terakhir akan diubah menjadi salah satu angka yang ada pada kunci 1. Sebaliknya, jika biner pesan rahasia adalah 0, maka digit terakhir diubah menjadi salah satu angka yang ada pada kunci 0. Pemilihan angka yang ada pada array kunci tersebut berdasarkan angka yang terdekat dari digit terakhir nilai piksel asli yang akan dimodifikasi. Sehingga tidak mengubah kualitas citra secara signifikan. Ilustrasi fase ini dapat dilihat pada gambar 3.

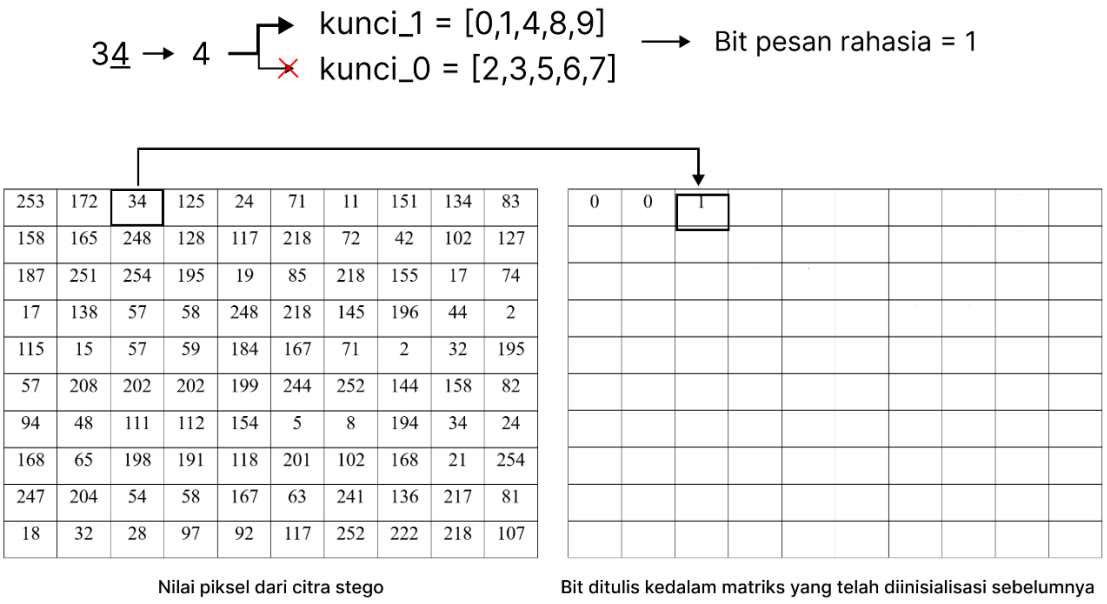


Gambar 3. Ilustrasi Penyisipan

e. Fase Ekstraksi

Proses ekstraksi data hampir sama dengan proses penyisipan. Proses ini juga mengandalkan digit terakhir dari nilai piksel untuk menentukan bit pesan rahasia. Pertama dari citra stego dilakukan pengambilan nilai piksel yang akan digunakan untuk proses selanjutnya. Lalu dilakukan pencocokan digit terakhir dari nilai piksel dengan dua array kunci yang telah disusun sebelumnya, yaitu kunci_1 dan kunci_0. Jika digit terakhir dari nilai piksel merupakan salah satu anggota dari kunci_1, maka bit pesan rahasia adalah 1. Begitu juga sebaliknya, jika digit terakhir merupakan salah satu anggota dari kunci_0, maka bit pesan rahasia adalah 0. Proses ini dilakukan secara berulang mulai dari piksel kiri atas sampai kanan bawah secara berurutan. Sehingga nantinya bit yang didapat akan dituliskan kedalam matriks yang sudah diinisialisasi sebelumnya. Ilustrasi proses ini dapat dilihat pada Gambar 4.

Selanjutnya, bit biner yang sudah diekstrak nantinya akan diubah kedalam karakter yang akhirnya membentuk pesan rahasia yang diambil dari citra stego. Proses ini memastikan bahwa data yang tersembunyi dapat diesktrak dengan benar menggunakan mekanisme kunci yang telah ditetapkan.



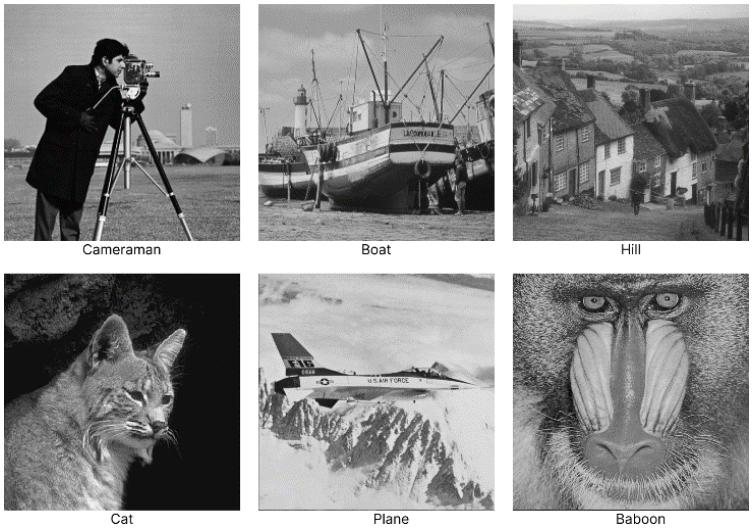
Gambar 4. Ilustrasi Ekstraksi Pesan Rahasia

HASIL DAN PEMBAHASAN

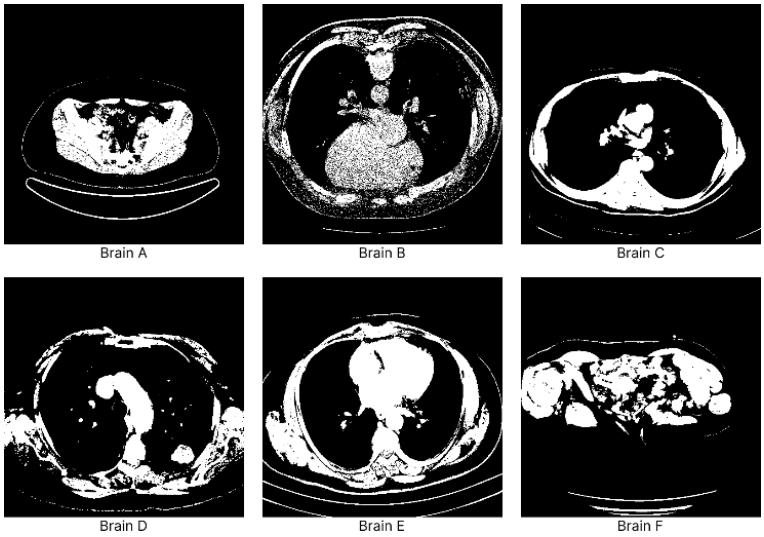
3.1 Skenario Pengujian

Pada pengujian tingkat distorsi yang terjadi pada citra akibat proses steganografi, metriks PSNR digunakan sebagai metode yang sudah diusulkan sebelumnya untuk mengukur kualitas citra stego. Pengujian dilakukan dengan menggunakan dua jenis citra, yaitu citra general dan citra medical, masing-masing berjumlah 6 buah citra berukuran 512 x 512. Semua citra diubah kedalam bentuk grayscale lalu disisipkan payload dengan ukuran yang bervariasi. Juga dilakukan pengujian kualitas citra dengan parameter alpha yang berbeda-beda.

pada pengujian variasi alpha, digunakan satu jenis payload dengan ukuran 262,14 Kb. Yang mana merupakan ukuran maksimal yang dapat ditampung oleh citra berukuran 512 x 512, payload dapat dilihat pada tabel 1. Sementara pada pengujian variasi payload digunakan 11 jenis payload dengan ukuran yang berbed, payload dapat dilihat pada tabel 2. Semua payload berisi angka random dengan bilangan minimal 1 dan maksimal 9 dengan jumlah digit tergantung dengan ukuran payload.



Gambar 5. Citra General



Gambar 6. Citra Medical

Tabel 1. Jenis Payload Pada Pengujian Variasi Alpha

Ukuran	Isi	Jumlah digit
262 Kb	Angka 1 sampai 9	32768

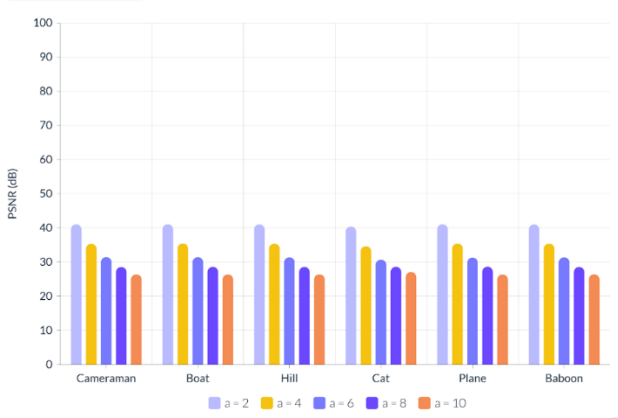
Tabel 2. Jenis Payload Pada Pengujian Variasi Ukuran Payload

Ukuran	Isi	Jumlah digit
1Kb	Angka 1 sampai 9	125
10Kb	Angka 1 sampai 9	1250
20Kb	Angka 1 sampai 9	2500
30Kb	Angka 1 sampai 9	3750
40Kb	Angka 1 sampai 9	5000
50Kb	Angka 1 sampai 9	6250
60Kb	Angka 1 sampai 9	7500
70Kb	Angka 1 sampai 9	8750
80Kb	Angka 1 sampai 9	10000
90Kb	Angka 1 sampai 9	11250
100Kb	Angka 1 sampai 9	12500

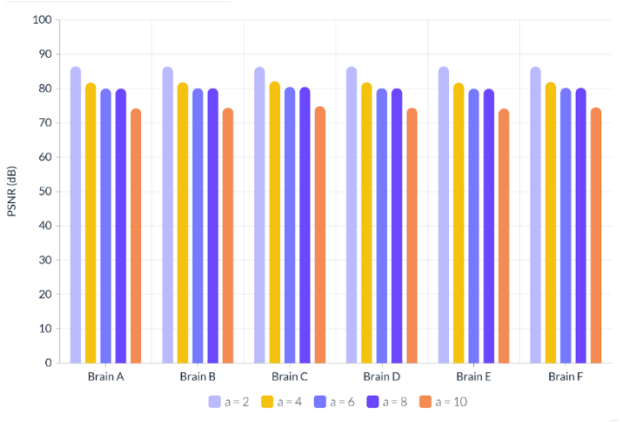
3.2 Implementasi

Parameter alpha digunakan dalam proses penyisipan untuk menggeser nilai piksel yang merupakan bagian dari metode Histogram Shifting. Hasil pengujian menunjukkan bahwa semakin tinggi nilai alpha, skor PSNR cenderung menurun. Dari diagram pada gambar 7 mengindikasikan jika parameter alpha memberikan pengaruh yang cukup signifikan terhadap penurunan kualitas citra, dibuktikan dengan nilai skor PSNR rata-rata menurun sebanyak 10% di setiap kenaikan alpha. Hal ini menunjukkan bahwa peningkatan nilai alpha berkontribusi menghasilkan distorsi yang cukup banyak.

Hasil yang serupa didapatkan pada pengujian alpha pada citra medical. Ini mengindikasikan bahwa penggunaan alpha yang lebih tinggi dapat menghasilkan distorsi yang lebih besar pada citra stego. Hal ini sudah pasti terjadi mengingat alpha berpengaruh langsung terhadap nilai piksel. Tetapi dilihat dari diagram pada gambar 8. citra medical cenderung menghasilkan skor PSNR yang lebih tinggi rata-rata 50% berbanding dengan citra general. Hal ini menandakan jika citra medical memiliki toleransi yang lebih baik terhadap proses steganografi yang menghasilkan distorsi pada citra [1].



Gambar 7. Diagram Hasil Pengujian Variasi Alpha Citra General

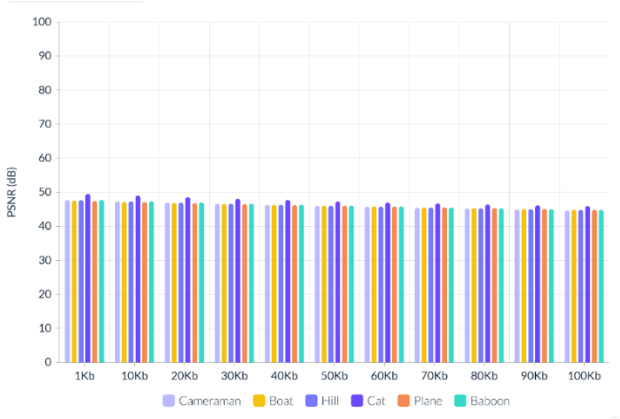


Gambar 8. Diagram Hasil Pengujian Variasi Alpha Citra Medical

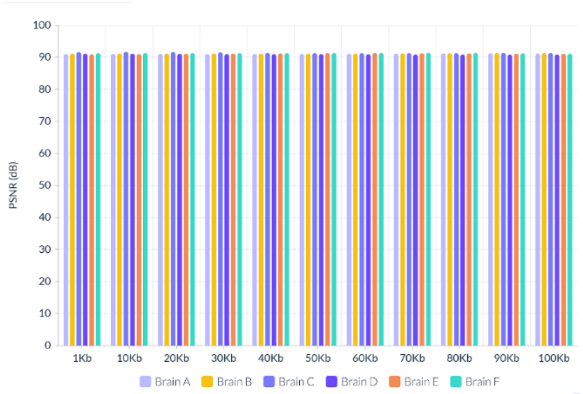
Pengujian selanjutnya dilakukan dengan menyisipkan payload dengan besaran yang bervariasi. Sebanyak sebelas payload digunakan pada pengujian ini, yaitu: 1Kb, 10Kb, 20Kb, 30Kb, 40Kb, 50Kb, 60Kb, 70Kb, 80Kb, 90Kb, dan 100Kb diujikan pada citra general dan citra medical. Pengujian ini bertujuan untuk mengetahui sejauh mana kapasitas payload yang disisipkan mempengaruhi kualitas citra stego. Skor PSNR tetap digunakan sebagai acuan.

Diagram pada gambar 9 Menunjukkan adanya penurunan kualitas citra seiring dengan peningkatan ukuran payload rata-rata sebanyak 2%. Hal ini dikarenakan semakin banyak bit pesan yang disisipkan, semakin besar distorsi yang dihasilkan pada citra karena setiap bit data yang disisipkan akan mengubah nilai piksel. Namun penurunan kualitas yang terjadi tidak signifikan dan nilai skor PSNR tetap pada level yang dapat diterima, artinya algoritma steganografi yang diusulkan sesuai untuk penggunaan penyisipan payload besar maupun kecil.

Hal yang menarik didapat dari hasil pengujian variasi payload pada citra medical pada gambar 10. Hasil menunjukkan bahwa citra-citra medis mampu mempertahankan skor PSNR yang stabil bahkan ketika ukuran payload yang disisipkan kedalam citra semakin besar. Ditunjukkan dengan nilai skor PSNR yang dihasilkan selalu berada diatas 90 dB. menandakan bahwa citra-citra medis sesuai untuk penyisipan pesan tanpa mengorbankan kualitas visual. Hal ini disebabkan oleh distribusi nilai piksel yang lebih merata pada citra medis, membuat lebih toleran terhadap proses penyisipan pesan rahasia. Citra medical memiliki lebih banyak piksel hitam dan variasi warna piksel yang sedikit, hal ini membuat citra menjadi toleran terhadap perubahan [1].



Gambar 9. Diagram Hasil Pengujian Variasi Alpha Citra Medical



Gambar 10. Diagram Hasil Pengujian Variasi Alpha Citra Medical

KESIMPULAN

Pentingnya steganografi sebagai metode keamanan digital tidak dapat diabaikan, terutama dalam konteks perlindungan informasi rahasia dan data sensitif. Steganografi adalah salah satu teknik penyembunyian data. Dibandingkan dengan metode lain seperti enkripsi, informasi yang dilindungi tidak terlihat pada media sampul. Penyembunyian data memungkinkan kita untuk merahasiakan informasi tanpa menimbulkan kecurigaan bahwa ada informasi yang kita rahasiakan.

Hasil pengujian alpha membuktikan adanya dampak yang signifikan dari parameter alpha terhadap kualitas citra stego. Peningkatan nilai alpha secara signifikan meningkatkan distorsi yang terlihat pada citra stego. Hal ini memberi gambaran jelas tentang sensitivitas algoritma terhadap perubahan parameter alpha. Analisis PSNR pada pengujian variasi alpha juga menunjukkan penurunan skor yang signifikan ketika nilai alpha dinaikkan. Pemilihan nilai alpha yang kecil akan memberikan kualitas citra yang lebih baik.Hasil pengujian payload menunjukkan bahwa metode yang diusulkan mampu mempertahankan kualitas citra pada berbagai variasi payload. Meskipun terdapat penurunan skor PSNR seiring dengan peningkatan payload, namun hasil tersebut berada dalam kisaran yang dapat diterima. Oleh karena itu, algoritma ini dapat dianggap efektif dalam menyisipkan pesan rahasia tanpa merusak kualitas citra.

Bahkan terdapat temuan yang menarik pada hasil pengujian. Algoritma mampu mempertahankan skor PSNR yang stabil pada citra medical, bahkan ketika payload ditingkatkan. Citra medical secara konsisten menunjukkan kualitas yang baik setelah disisipkan dengan variasi ukuran payload. Temuan ini merupakan hal yang positif terkait kemampuan algoritma untuk mempertahankan kualitas citra, khususnya pada citra medical.

Penelitian ini merinci penggunaan algoritma penyisipan yang diusulkan oleh penulis sebagai suatu pendekatan steganografi. Sebagai dasar dari keberhasilan algoritma, hasil yang didapat adalah kemampuannya untuk mempertahankan kualitas citra, terutama pada citra medis. Dengan parameter yang dioptimalkan, algoritma mampu memberikan tingkat keamanan yang baik sambil tetap memperlihatkan kejelasan visual yang optimal.

DAFTAR PUSTAKA

[1] C. C. Islamy, T. Ahmad, and R. M. Ijtihadie, "Reversible data hiding based on histogram and prediction error for sharing secret data," *Cybersecurity*, vol. 6, no. 1, Dec. 2023, doi: 10.1186/s42400-023-00147-y. https://cybersecurity.springeropen.com/articles/10.1186/s42400-023-00147-y

[2] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075. https://www.sciencedirect.com/science/article/abs/pii/S0925231218312591?via%3Dihub

[3] D. Artz, "Digital Steganography: Hiding Data within Data," 2001. [Online]. Available: http://computer.org/internet/

[4] F. Al-Shaarani and A. Gutub, "Securing matrix counting-based secret-sharing involving crypto steganography," *Journal of King Saud University - Computer and Information Sciences*, 2021, doi: 10.1016/j.jksuci.2021.09.009. https://www.sciencedirect.com/science/article/pii/S1319157821002603?via%3Dihub

[5] Adel Almohammad and Gheorghita Ghinea, *Stego Image Quality and the Realiability of PSNR*. 2010.

[6] 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. doi: 10.1016/j.sigpro.2009.08.010. https://www.sciencedirect.com/science/article/abs/pii/S0165168409003648?via%3Dihub

[7] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, Aug. 2003, doi: 10.1109/TCSVT.2003.815962. https://ieeexplore.ieee.org/document/1227616

[8] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–361, Mar. 2006, doi: 10.1109/TCSVT.2006.869964. https://ieeexplore.ieee.org/document/1608163

[9] H. Cherifi *et al.*, "Histogram Shifting as a Data Hiding Technique: An Overview of Recent Developments," 2011.

[10] C. F. Lee, H. L. Chen, and H. K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion," *Journal of Systems and Software*, vol. 83, no. 10, pp. 1864–1872, Oct. 2010, doi: 10.1016/j.jss.2010.05.078. https://www.sciencedirect.com/science/article/abs/pii/S0164121210001585?via%3Dihub

[11] T. C. Lu, C. C. Chang, and Y. H. Huang, "High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting," *Multimed Tools Appl*, vol. 72, no. 1, pp. 417–435, 2014, doi: 10.1007/s11042-013-1369-0. https://link.springer.com/article/10.1007/s11042-013-1369-0

[12] H. C. Huang, Y. H. Chen, and Y. Y. Lu, "Histogram-based difference expansion for reversible data hiding with content statistics," in *Proceedings - 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2011*, 2011, pp. 37–40. doi: 10.1109/IIHMSP.2011.38. https://ieeexplore.ieee.org/document/6079528

[13] C. C. Islamy and T. Ahmad, "Improving the quality of stego image using prediction error and histogram modification," *International Journal of Intelligent Engineering and Systems*, vol. 12, no. 5, pp. 95–103, 2019, doi: 10.22266/ijies2019.1031.10. https://www.inass.org/2019/2019103110.pdf