A Novel LSB Image Steganography Modification: Bit Modification on RGB Image Component

[Modifikasi Steganografi Citra Metode Least Significant Bit Modifikasi Bit pada Komponen Citra RGB]

Yenni Seftiardiyah [1)], Mochamad Alfan Rosid [*,2)], Hamzah Setiawan [3)], Sukma Aji [4)]

[1, 2, 3, 4)]Program Studi Informatika, Universitas Muhammadiyah Sidoarjo, Indonesia

*Email Penulis Korespondensi: alfanrosid@umsida.ac.id

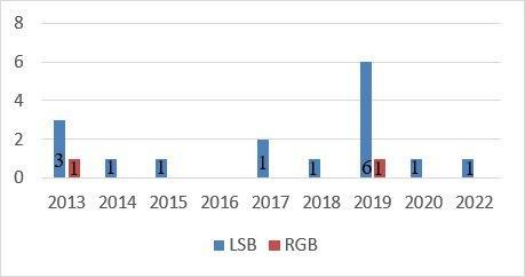
Abstract. *Image steganography is a method that involves composing hidden messages and embedding them into an image carrier. This ensures that only the sender and the receiver are know that the image contains a hidden message. This study refines the Least Significant Bit (LSB) method of image steganography by switching the least significant bit with the most significant bit and incorporating a hidden message bit in the process. The purpose of this study is to identify a new way to modify the approach of embedding messages from the least significant bit on Red, Green, and Blue (RGB) image components all the way up to the most significant bit. The findings of this study include an image comparison that is encoded with a secret message from the least significant bit all the way up to the most significant bit, then calculated using Mean Square Error (MSE), Peak Signal Noise Ratio (PSNR), Root Mean Square Error (RMSE), and Structural Similarity Index Metric (SSIM) to make a comparisons which stego-image that have a best result. This study found a new method that the best result of MSE, PSNR, RMSE and SSIM on the plane image on the 6th bit.*

Keywords *– Least Significant Bit; Steganography Modification; RGB Image Component*

Abstrak. *Steganografi gambar merupakan metode yang melibatkan penyisipan pesan tersembunyi dan memasukkannya ke dalam gambar pembawa. Ini memastikan bahwa hanya pengirim dan penerima yang tahu bahwa gambar tersebut berisi pesan tersembunyi. Penelitian ini melakukan percobaan dengan memodifikasi metode Least Significant Bit dengan menukar bit yang paling belakang hingga bit paling depan dengan bit pesan rahasia. Tujuan dari penelitian ini adalah untuk mengidentifikasi cara baru untuk melakukan penyisipan pesan rahasia hasil modifikasi dari metode Least Significant Bit pada komponen gambar Red, Green dan Blue (RGB). Temuan dari penelitian ini adalah perbandingan gambar pembawa dan gambar yang sudah disisipi pesan rahasia dari bit paling belakang hingga bit paling depan, kemudian dihitung menggunakan Mean Square Error (MSE), Peak Signal Noise Ratio (PSNR), Root Mean Square Error (RMSE), dan Structural Silimarity Index Metric (SSIM) untuk membuat perbandingan hasil stego-image mana yang paling baik hasilnya. Studi ini menemukan bahwa hasil perhitungan MSE, PSNR, RMSE dan SSIM terbaik berada pada gambar plane dengan penyisipan pada bit ke 6.*

Kata Kunci *– Least Significant Bit; Steganography Modification; RGB Image Component*

I. PENDAHULUAN



Gambar 1. Top Survey Artikel Tentang Steganografi Gambar

Terdapat masalah keamanan data penting bagi sejumlah besar pengguna yang mentransfer data secara teratur [1]. Ada banyak metode enkripsi yang berbeda sekarang sedang diteliti untuk mengenkripsi data agar lebih aman. Steganografi adalah salah satu sub bidang teknologi kriptografi yang berada di bawah rumpun penyisipan data[2]. Steganografi mengacu pada praktik menyembunyikan informasi rahasia dalam berbagai jenis media [3]. Gambar [4], [5], video [6], suara [7], [8], dan teks tertulis [9] [10] adalah semua jenis media yang berbeda [11]. Steganografi merupakan seni menambatkan pesan rahasia dalam media pembawa yang dapat digunakan untuk *decoding* pesan tersembunyi [12], [13], [14]. Steganografi dan kriptografi adalah metode yang dapat digunakan untuk memasukkan pesan rahasia dalam berbagai bentuk media [11], [15]. Operasi yang digunakan dalam metod

LSB ini adalah menyisipkan pesan rahasia di bit paling belakang sendiri pada gambar. Steganografi citra biasanya memanfaatkan komponen warna RGB pada citra karena kekuatan komponen RGB dalam pemrosesan citra digital.

Dengan menggunakan metode LSB, penulis melakukan penelitian di bagian RGB pada komponen gambar. Menurut temuan survey yang telah dilakukan, terdapat 54 artikel di bidang steganografi. Jumlah studi steganografi gambar yang menggunakan pendekatan LSB ditampilkan dalam gambar 1. Beberapa penelitian tersebut menggunakan metode LSB pada komponen gambar RGB. Metode LSB pada dasarnya adalah metode penyisipan pesan rahasia yang paling sederhana di antara semua metode penyisipan pesan dalam steganografi. Oleh karena itu, kebanyakan penelitian menggunakan metode ini secara berbeda dari algoritma yang mudah digunakan. Kode pseudocode untuk algoritma prosedur LSB ditunjukkan di bawah ini.

```
Input: text, carrier image
Output: stego-image
def data to binary:
        if type data == string:
                format to binary
        return to the process until it's done converted to binary
encode:
        define the secret key, then
        for pixel in value :
        pixel[x]=data to binary + insert binary message into it's own backmost bit in the image component, then
        update pixel values
        return to image
decode:
        input the stego-image
        for readable data in all bytes:
                read all bytes and find readable data
                if readable data is found, then
                break
        return to readable data
end
```

Penelitian tentang steganografi citra menggunakan pendekatan LSB populer pada tahun 2019, dengan enam publikasi. Namun, penelitian tentang steganografi menggunakan komponen gambar RGB jarang disebutkan, seperti terlihat pada gambar 1. penulis mengusulkan terobosan lain dalam memasukkan pesan ke dalam bit gambar. Secara khusus berubah dari bit ke-7 sampai bit 0 pada gambar, terutama pada komponen gambar RGB dengan bit pesan rahasia.

II. PENELITIAN TERKAIT DAN METODE

A. Penelitian Terkait

Penelitian yang dilakukan oleh Aditya Kumar Sahu dan Gandharba Swain [16] menggunakan modifikasi bit paling kanan dalam steganografi gambar, yang bertujuan untuk meningkatkan Peak Signal Noise Ratio (PSNR), meningkatkan Embedding Capacity (EC), menghindari Fall of Boundary Problem (FOPB), dan resistensi terhadap *salt and pepper noise* dan serangan RS.

Mohammed Mahdi Hashem [17] melakukan beberapa penelitian dengan maksud untuk meninjau steganografi gambar di berbagai domain spasial. Dalam penelitiannya, ia mencakup banyak pendekatan steganografi citra, baik secara geografis maupun transformasi domain, dan kemudian membandingkan temuan dari beberapa proyek penelitian. Penelitian ini memberikan hasil perbandingan dari hasil kerja berbagai peneliti lain sebelumnya mengenai tingkat keamanan, kapasitas, dan tingkat pesan rahasia tersembunyi.

Gambaran umum tentang nomeklatur dan taksonomi pola penyisipan tersembunyi diteliti oleh Luca Cavinglione [18]. Taksonomi sebelumnya diubah sebagai hasil dari penelitian ini, yang menghasilkan alat untuk semua domain steganographic, membuat diktinsi antara proses penyematan lebih eksplisit, dan menghasilkan representasi pola data tersembunyi.

Osama F. Abdel Wahab [19] melakukan penelitian pada metode steganografi, melakukan penelitian pada metode steganografi, yang melibatkan menyembunyikan pesan rahasia dalam gambar melalui penggunaan algoritma kompresi. Penelitiannya menggunakan dua pendekatan: yang pertama melibatkan penggunaan teknik LSB ke pesan rahasia tanpa mengenkripsikannya terlebih dahulu, dan yang kedua melibatkan penerapan teknik LSB ke pesan

rahasia setelah dienkripsi. Setelah itu, MSE dan PSNR dihitung untuk melakukan perbandingan antara kedua pendekatan.

Penelitian oleh Xiaoli Huan [20] menggambarkan adaptasi pendekatan baru utuk metode LSB. Metodologi baru ini memanfaatkan pemilihan bibit pada gambar asli untuk menghindari deteksi pada bagian gambar yang halus atau datar. Studi ini sampai pada kesimpulan bahwa metode yang digunakan memiliki kualitas visual yang baik seperti yang ditunjukkan oleh hasil dari PSNR yang lebih besar daripada PSNR gambar pembawa.

Studi steganografi menggunakan kriptosistem RSA untuk mengkodekan pesan untuk keamanan ekstra dilakukan oleh Ismael Martinez [21]. Metode ini adalah mengubah teks menjadi array bit dan disimpan dalam lapisan RGB pada gambar. Hasil penelitian ini adalah bahwa re-enkripsi independen dari citra pembawa.

Penelitian oleh Sara Farrag dan Wassim Alexan [22] studi tentang skema pesan aman lapis ganda adalah langkah awal adalah mengenkripsi menggunakan DES, CAST5 atau BlowFish, kemudian tahap kedua adalah data terenkripsi disembunyikan dalam gambar pembawa menggunakan metode LSB. Hasil penelitian ini adalah pengukuran nilai MSE, PSNR, dan SSIM dari gambar yang berisi pesan rahasia.

Mirza Abdur Razzaq [23] penelitian tentang enkripsi, steganografi dan teknik watermarking menggunakan keamanan campuran. Enkripsi yang digunakan dalam penelitian ini adalah teknik enkripsi XOR dan metode LSB, kemudian gambar ditandai wwatermark.

Metode steganografi berbasis domain spasial baru diusulkan oleh Marwa M. Emam [24] dengan mengacak pesan rahasia dan menanamkan dalam piksel gambar sampul menggunakan Pseudo Random Number Generation (PNRG). Hasil dari metode ini adalah perhitungan menggunakan Kapasitas Kebisingan Maksimum dan PSNR pada gambar yang berisi pesan rahasia.

Metode baru yang dikembangkan oleh Joyshree Nath [25] menggunakan algoritma yang diusulkan oleh Nath et al [26] untuk menghasilkan metode randomisasi baru dalam enkripsi teks. Metode ini menghasilkan algoritma yang dapat menentukan nomor acak dan nomor enkripsi dari kunci teks yang disediakan untuk menciptakan metode enkripsi watermarking yang paling aman.

B. Landasan Teori

Steganografi adalah topik kajian yang berfokus pada praktik menyembunyikan komunikasi untuk mencegah pihak-pihak yang tidak berwenang [27]. Steganografi adalah sub bidang kriptografi. Kriptografi, di sisi lain, adalah metode untuk menyembunyikan transmisi pesan dengan meminta bantuan cipher dan decipher untuk menguraikan informasi tersembunyi [28].

Kata steganografi berasal dari bahasa Yunani steganos, yang berarti “tersembunyi”, dan graphien adalah “menulis”. Dapat disimpulkan bahwa steganografi adalah “penulisan pesan tersembunyi”. Steganografi dapat dgunakan pada media digital seperti video, gambar, suara, dan teks. Konsep inti steganografi adalah menyembunyikan pesan rahasia di media sehingga orang ketiga tidak tahu bahwa media berisi pesan rahasia. Penelitian ini berfokus pada steganografi gambar yang tertanam dalam komponen gambar RGB. Ada beberapa komponen warna dalam gambar, secara khusus akan dijelaskan di bawah ini.

- Red, Green, Blue (RGB): ini adalah warna utama pada layar monitor. RGB dihasilkan dari cahaya monitor dan merupakan “Additive Color System” [29], yang berarti semakin banyak warna digabungkan, semakin tinggi intensitasnya.
- Cyan, Magenta, Yellow, Black (CMYK): pada komponen warna, CMYK seringkali digunakan untuk percetakan karena CMYK merupakan “ Subtractive Color Model” [30], yang berarti semakin banyak warna yang digabungkan dan semakin tinggi intensitasnya, semakin sedikit intensitas cahaya yang dihasilkan. CMYK memiliki intensitas yang lebih buram daripada RGB. Jadi, ketika menggabungkan warna dengan intensitas yang sama, ia akan mendekati warna hitam.
- Hue, Saturation, Value (HSV): komponen ini lebih diarahkan ke pengaturan gelap dan terang dalam gambar. Konsep HSV adalah bahwa semakin tinggi tingkat saturasi, warna murni akan muncul. Sedangkan jika saturasi sedikit, warna akan mendekati warna abu-abu [30].

Penjelasan diatas menunjukkan bahwa komponen wara RGB menghasilkan warna terbaik di layar monitor [29]. Penelitian ini mengambil komponen gambar RGB karena intensitasnya lebih terang daripada CMYK dan HSV, sehingga memungkinkan gambar yang berisi pesan rahasia tidak diketahui dengan pihak ketiga karena mirip dengan gambar pembawa. Perbandingan intensitas antara gambar pembawa dan gambar yang berisi pesan rahasia (stego-image) dapat dihitung menggunakan rumus matematika, dengan rumus sebagai berikut:

- Mean Square Error (MSE)

  MSE mengukur rata-rata kesalahan kuadrat yang paling sering digunakan dalam metrik pengukuran kualitas gambar. Dalam pemrosesan citra digital, terutama dalam steganografi citra, MSE digunakan untuk membandingkan nilai rata-rata kesalahan kuadrat antara citra pembawa dan citra yang berisi pesan rahasia. Jika nilai MSE mendekati 0, semakin baik nilainya. Rumus MSE dijelaskan di bawah ini[31], [32]:

$$MSE = \frac{1}{MN} \sum_{X=0}^{M} \sum_{Y=1}^{N} \left[C(x,y) - \hat{C}(x,y) \right]^2$$

Dimana,
X dan Y = koordinat gambar
M dan N = dimensi gambar
$\hat{C}(x,y)$ = gambar yang berisi pesan rahasia (stego-image)
C(x,y) = carrier image

- Peak Signal Noise Ratio (PSNR)

  PSNR digunakan untuk membandingkan kualitas gambar dari gambar pembawa dengan gambar yang berisi pesan rahasia; semakin baik nilai PSNR yang dihasilkan, semakin baik kualitas gambar, semakin mirip gambar stego dengan gambar pembawa [33]. PSNR diukur dalam satuan dB (decibel) [31].

$$PSNR = 10 \log(10) \left(\frac{MAXVAL^2}{MSE} \right)$$

  Dimana,
  PSNR = Peak Signal Noise Ratio (dB)
  MAXVAL = nilai maksimum dalam piksel, dimana 255 [34]

- Root Mean Square Error (RMSE)
  RMSE adalah akar kuadrat pengukuran dari MSE, yang berarti laju perhitungannya lebih akurat daripada MSE [14]; semakin kecil nilai RMSE, semakin akurat perhitungannya.

$$RMSE = \sqrt{MSE}$$

  Dimana,
  RMSE = Root Mean Square Error
  MSE = Mean Square Error

- Structural Similarity Index Metric (SSIM)

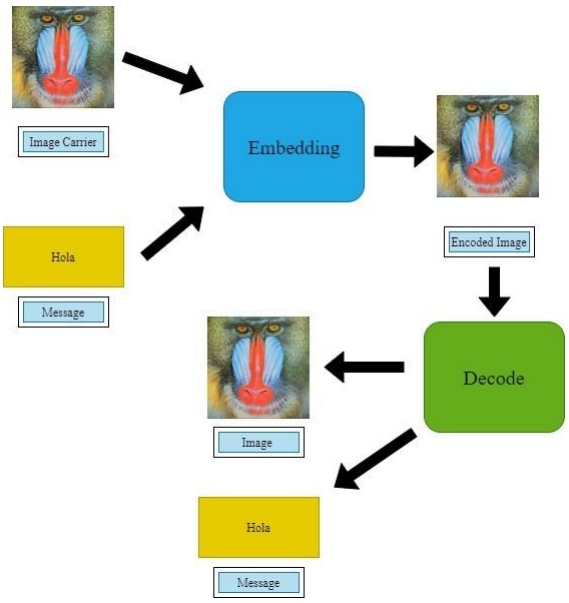
  SSIM adalah metode perhitungan untuk membandingkan kesamaan dua gambar; dalam metode ini, degredasi gambar dapat menyebabkan perubahan presepsi. SSIM dalam metode perhitungan memiliki beberapa faktor, misalnya masking pencahayaan, masking kontras, dan lain-lain[31].

$$SSIM = \frac{(2\mu X \mu Y + c1)(2\sigma XY + c2)}{(\mu X + \mu Y + C1)(\mu X^2 + \mu Y^2 + C2)}$$

  Dimana,
  μ, σ = standard deviasi gambar asli X dan gambar yang mengandung pesan rahasia Y
  XY = kovarian dari X dan Y
  C1 dan C2 = konstanta untuk mencegah ketidakstabilan numerik [32]

C. Metodologi

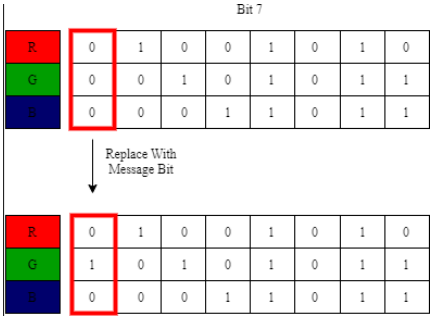
Secara umum, pendekatan steganografi gambar melibatkan proses inti yang disebut sebagai embedding dan decoding. Decoding adalah tindakan membaca pesan rahasia yang telah tertanam dalam media, sedangkan embedding adalah proses memasukkan pesan tersembunyi di dalam media. Embedding adalah prosedur yang menyisipkan pesan rahasia.



Gambar 2. Proses Steganografi Gambar

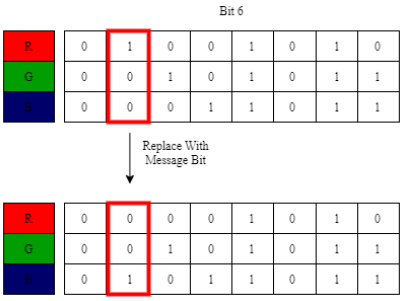
Gambar 2 menjelaskan aliran penyisipan dan membaca pesan dalam steganografi gambar [35]. Steganografi gambar memiliki media gambar yang disebut gambar pembawa (carrier image) dan teks. Teks adalah pesan rahasia yang nantinya akan disisipkan dalam gambar pembawa. Keluaran dari proses penyisipan akan merilis gambar yang berisi pesan rahasia di dalamnya. Metode penyisipan pesan rahasia yang paling populer saat ini adalah metode yang menyisipkan pesan pada bit paling belakang sendiri atau LSB. Proses penyisipan pada LSB akan dijelaskan pada gambar 3.

Gambar 3. Penyisipan Metode LSB

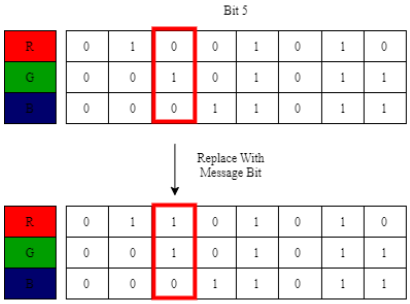


Gambar 4. Modifikasi di Bit 7

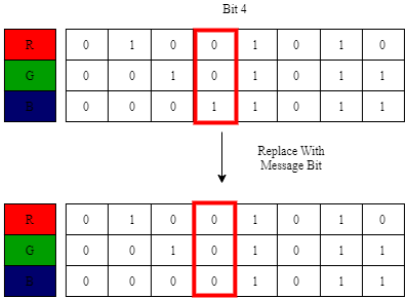
Karakteristik pada Metode LSB adalah memasukkan pesan di bit paling akhir [36]. Metode ini sering digunakan karena dianggap cukup sederhana untuk melakukan penyisipan sebuah pesan di gambar dibandingkand dengan metode lain.



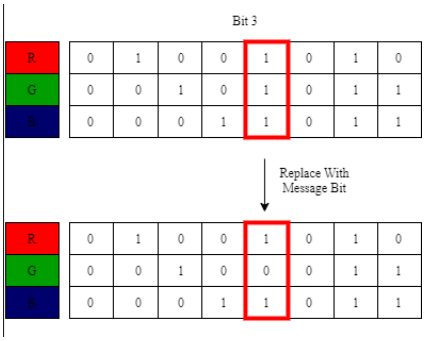
Gambar 5. Modifikasi di Bit 6



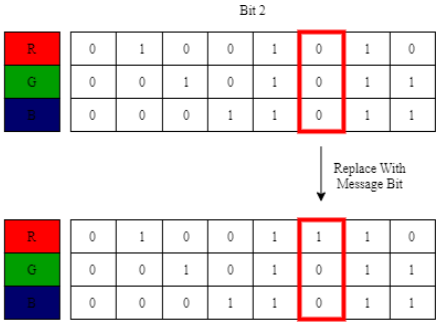
Gambar 6. Modifikasi di Bit 5



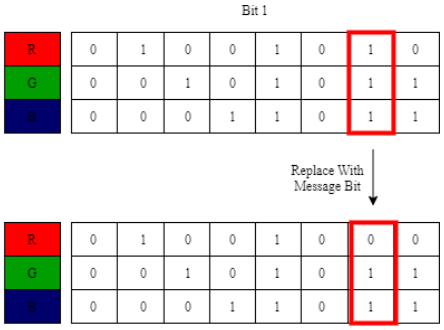
Gambar 7. Modifikasi di Bit 4



Gambar 8. Modifikasi di Bit 3



Gambar 9. Modifikasi di Bit 2



Gambar 10. Modifikasi di Bit 1

Gambar 11. Modifikasi di Bit 0

Dasar dari penelitian ini adalah menggunkan metode LSB, kemudian kami mengusulkan teknik penyisipan baru dengan memdifikasi metode LSB dengan memindahkan penyisipan pesan dari bit ke 7 sampai bot 0. metode modifikasi LSB yang dimaksud dijelaskan pada gambar 4.

Bit ke 7 disisipkan oleh bit pesan rahasia yang ditunjukkan pada gambar 4. Percobaan selanjutnya adalah memasukkan bit pesan rahasia pada bit ke 6 gambar. Bit ke 6 sudah disisipi oleh pesan rahasia. Setelah mendapatkan hasil gambar penyisipan dari bit ke 6 yang pada gambar 5, percobaan selanjutnya akan diulang pada bit ke 5. bit k 5 dimodifikasi dengan bit pesan rahasia yang ditunjukkan pada gambar 6. Setelah menghasilkan

gambar stegano, percobaan penyisipan dilakukan pada bit ke 4. Bit ke 4 disisipi dengan bit pesan rahasia yang ditunjukkan pada gambar 7. Percobaan dilakukan kembali pada bit ke 3. Bit ke 3 disisipi dengan bit pesan rahasia yang dijelaskan pada gambar. Setelah medapatkan keluaran gambar stegano, percobaan selanjutnya adalah memasukkan bit pesan rahasia ke bit ke 2.

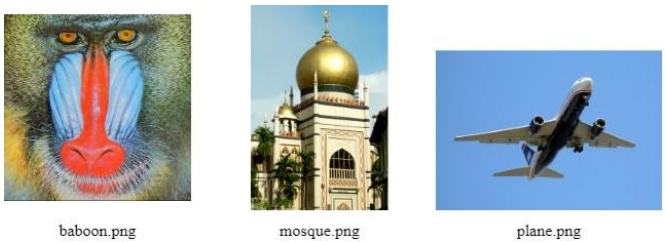
Proses embedding pada bit ke 2 ditunjukkan pada gambar 9. Percobaan selanjutnya adalah memasukkan pesan rahasia pada bit 1. Bit 1 disisipi dengan pesan rahasia ditunjukkan pada gambar 10. Metode eksperimental untuk memasukkan bit terakhir adalah pada bit 0. Bit 0 disisipi oleh bit pesan rahasia, ditunjukkan pada gambar 11. Hasil akhir dari metode ini adalah beberapa gambar yang telah dimasukkan pesan dari bit ke 7 sampai bit ke 0, kemudian dihitung MSE, PSNR, RMSE, dan SSIM yang kemudian akan menentukan penyisipan pada bit mana yang memiliki hasil terbaik, atau dapat dikatakan mendekati dengan gambar pembawa.

III. HASIL DAN PEMBAHASAN

Hasil akhir dari metode ini menghasilkan 24 gambar dari 3 gambar pembawa dengan pesan yang sudah tersisip ke dalam gambar. Untuk mencapai hasil terbaik, pendekatan metodologi digunakan.

A. Perbandingan Gambar Pembawa

Gambar pembawa pada penelitian ini menggunakan tiga gambar, yaitu baboon.png [37], plane.png [38], and mosque.png [39].



Gambar 12. Gambar Pembawa

Gambar 12 merupakan gambar pembawa yang akan digunakan dalam penelitian ini. Ketiga gambar tersebut dimasukkan pesan rahasia yang bertuliskan “hola”.

B. Proses

Proses awal untuk menanamkan pesan rahasia pada tiga gambar pembawa dijelaskan pada gambar 4 hingga gambar 11. Setiap gambar pembawa menghasilkan delapan gambar yang berisi pesan rahasia yang dimasukkan dalam setiap bit (bit 7 sampai bit 0) sehingga gambar keluaran yang sudah tersisipi pesan rahasia adalah 24 gambar, setelah memperoleh 24 gambar stego, langkah selanjutnya adalah menghitung menggunakan rumus MSE, RMSE, PSNR, dan SSIM untuk membandingkan kesamaan dari gambar pembawa.

Hasil perhitungan terbaik pada gambar baboon terletak di baboon_bit4.png yang ditunjukkan pada tabel 1 dengan hasil 52.75 pada nilai PSNR, 0.344 MSE, 0.0042 RMSE dan 0.9999978 pada SSIM. Tabel selanjutnya akan menjelaskan nilai terbaik pada gambar plane.png. Gambar plane.png memiliki hasil terbaik pada gambar plane_bit6.png yang memiliki nilai PSNR 62.47, MSE 0.036, RMSE 0.011 dan SSIM 0.9999993. Tabel selanjutnya adalah menjelaskan nilai MSE, PSNR, RMSE, dan SSIM gambar mosque.png.

Nilai terbaik pada gambar mosque.png adalah terletak di mosque_bit6.png dengan nilai PSNR adalah 57.61, MSE 0.112, RMSE 0.0019 dan SSIM 0.9999986.

Perhitungan MSE, PSNR, RMSE dan SSIM menunjukkan bahwa semua gambar yang disisipi pesan rahasia mendekati gambar pembawa, sedangan MSE dan RMSE mendekati 0. PSNR dari semua gambar berada diatas 30 dB, sementara nilai SSIM dari semua gambar mendekati 1.

Pada bagian ini, temuan penelitian dibahas sekaligus dijelaskan secara menyeluruh. Hasil akhir dapat ditampilkan dalam tabel, grafik, angka, dan format lain yang sederhana untuk memudahkan pembaca [14], [15]. Terdapat banyak cara untuk menjelaskan topik.

Table 1. Hasil Kalkulasi Gambar Baboon

Figure	MSE	PSNR	RMSE	SSIM
Baboon_bit7.png	0.668228	49.881555	0.005907	0.999972
Baboon_bit6.png	0.537043	50.830710	0.005295	0.999975
Baboon_bit5.png	0.416112	51.938698	0.004661	0.999978
Baboon_bit4.png	0.344904	52.753813	0.004244	0.999978
Baboon_bit3.png	0.387181	52.251656	0.004496	0.999976
Baboon_bit2.png	0.350458	52.684434	0.004278	0.999976
Baboon_bit1.png	0.512710	51.032080	0.005174	0.999972
Baboon_bit0.png	0.563878	50.618949	0.005426	0.999970

Table 2. Hasil Kalkulasi Gambar Plane

Figure	MSE	PSNR	RMSE	SSIM
Plane_bit7.png	0.079411	59.131948	0.001686	0.999993
Plane_bit6.png	0.036737	62.479712	0.001146	0.999994
Plane_bit5.png	0.047603	61.354402	0.001305	0.999994
Plane_bit4.png	0.068743	59.758501	0.001568	0.999993
Plane_bit3.png	0.076416	59.298906	0.001654	0.999993
Plane_bit2.png	0.093735	58.411763	0.001832	0.999993
Plane_bit1.png	0.163304	56.000814	0.002418	0.999993
Plane_bit0.png	0.173980	55.725806	0.002495	0.999993

Table 3. Hasil Kalkulasi Gambar Mosque

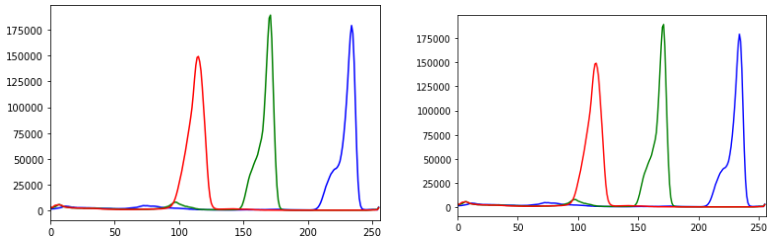
Figure	MSE	PSNR	RMSE	SSIM
Mosque_bit7.png	0.140382	56.657658	0.002227	0.999987
Mosque_bit6.png	0.112649	57.613505	0.001995	0.999986
Mosque_bit5.png	0.158205	56.138595	0.002364	0.999985
Mosque_bit4.png	0.206538	54.980792	0.002701	0.999984
Mosque_bit3.png	0.204838	55.016686	0.002690	0.999984
Mosque_bit2.png	0.360032	52.567380	0.003567	0.999984
Mosque_bit1.png	0.581560	50.484852	0.004533	0.999983
Mosque_bit0.png	0.610727	50.272329	0.004646	0.999983

Badshah dalam penelitiannya, menyatakan bahwa jika nilai PSNR di bawah 30 dB, citra tidak dapat digunakan untuk analisis lebih lanjut karena tidak mendekati citra pembawa. Jika gambar memiliki nilai PSNR diatas 30 dB, maka memiliki kesamaan pada gambar pembawa [21]. Berdasarkan gambar baboon.png, hasil terbaik dari penyisipan pesan berada di bit ke 4, sedangkan plane.png dan mosque.png berada di bit ke 6. Jika nilai indeks SSIM mendekati 1, maka gambar stego hampir mirip dengan gambar pembawa [40], sementara untuk nilai MSE dan RMSE, semakin kecil nilainya atau mendekati 0 maka semakin baik hasilnya[41], [42].

C. Perbandingan Secara Fisik Antara Stego-Image dan Gambar Pembawa

Diantara sambar stego yang memiliki hasil paling baik pada perhitungan MSE, PSNR, RMSE dan SSIM dimana yang mendekati gambar pembawa terdapat pada gambar plane_bit6.png, sehingga hampir tidak ada perbedaan fisik dengan gambar pembawa. Perbandingan secara fisik antara gambar stego plane_bit6.png dan gambar pembawa plane.png dapat dilihat pada gambar 12.

Gambar 13. Plane.png (Kiri) dan Plane_bit6.png (Kanan)



Gambar 14. Histogram Plane.png (Kiri) dan Plane_bit6.png (Kanan)

Gambar 13 menampilkan grafik histogram plane.png sebagai gambar pembawa dan plane_bit6.png sebagai gambar yang berisi pesan rahasia pada bit 6. Dapat dilihat dengan jelas bahwa tidak ada perbedaan yang signifikan antara gambar stego dan gambar pembawa.

V. SIMPULAN

Dalam makalah ini, kami mengusulkan teknik penyisipan baru untuk steganografi gambar. Teknik eksperimen yang digunakan dalam penelitian ini adalah dengan menyisipkan pesan rahasia dari bit paling kiri (bit 7) ke bit paling kanan (bit 0) dengan menggunakan tiga sampel gambar: baboon.png, plane.png, dan mosque.png. Ketiga gambar sampel tersebut menghasilkan 24 gambar yang sudah tersisipi pesan rahasia, kemudian perhitungan menggunakan rumus MSE, PSNR, RMSE, dan SSIM digunakan untuk mengetahui metode penyisipan pada bit mana yang memiliki hasil perhitungan terbaik. Hasil terbaik terdapat pada gambar plane_bit6.png dimana penyisipan dilakukan di bit ke 6. Kami juga membandingkan bentuk fisik gambar plane.png dan plane_bit6.png menggunakan histogram untuk membandingkan apakah ada perbedaan secara fisik antara gambar pembawa dan gambar stego. Hasil perbandingan secara fisik dan histogram menunjukkan tidak ada perbedaan secara signifikan diantara kedua gambar.

Penelitian selanjutnya disarankan untuk melakukan uji derau pada gambar yang disisipkan pesan rahasia menggunakan metode yang kami usulkan, kemudian diitung kembali menggunakan rumus MSE, PSNR, RMSE, dan SSIM sebagai acuan perbandingan hasil ketahanan pada serangan derau.

REFERENSI

[1] A. Sajid Ansari, M. Sajid Mohammadi, and M. Tanvir Parvez, “A Comparative Study of Recent Steganography Techniques for Multiple Image Formats,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 11–25, 2019, doi: 10.5815/ijcnis.2019.01.02.

[2] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, “A novel image steganography technique based on quantum substitution boxes,” *Opt. Laser Technol.*, vol. 116, no. February, pp. 92–102, 2019, doi: 10.1016/j.optlastec.2019.03.005.

[3] M. Garg, “A Novel Text Steganography Technique Based on Html Documents,” *Int. J. Adv. Sci. Technol.*, vol. 35, pp. 129–138, 2011.

[4] X. Li, W. Zhang, B. Ou, and B. Yang, “A brief review on reversible data hiding: Current techniques and future prospects,” *2014 IEEE China Summit Int. Conf. Signal Inf. Process. IEEE ChinaSIP 2014 - Proc.*, pp. 426–430, 2014, doi: 10.1109/ChinaSIP.2014.6889278.

[5] B. J. Mohd, S. Abed, B. Na’ami, and T. Hayajneh, “Hierarchical steganography using novel optimum quantization technique,” *Signal, Image Video Process.*, vol. 7, no. 6, pp. 1029–1040, 2013, doi: 10.1007/s11760-012-0301-9.

[6] M. Marsaline Beno, A. George, I. R. Valarmathi, and S. M. Swamy, “Hybrid optimization model of video steganography technique with the aid of biorthogonal wavelet transform,” *J. Theor. Appl. Inf. Technol.*, vol. 63, no. 1, pp. 190–199, 2014.

[7] P. Pathak, A. K. Chattopadhyay, and A. Nag, “A new audio steganography scheme based on location selection with enhanced security,” *1st Int. Conf. Autom. Control. Energy Syst. - 2014, ACES 2014*, pp. 1–4, 2014, doi: 10.1109/ACES.2014.6807979.

[8] M. Tayel, A. Gamal, and H. Shawky, “A proposed implementation method of an audio steganography technique,” *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2016-March, no. 3, pp. 180–184, 2016, doi: 10.1109/ICACT.2016.7423320.

[9] A. Odeh, K. Elleithy, and M. Faezipour, “Steganography in text by using MS word symbols,” *Proc. 2014 Zo. 1 Conf. Am. Soc. Eng. Educ. - “Engineering Educ. Ind. Involv. Interdiscip. Trends”, ASEE Zo. 1 2014*, no. April, 2014, doi: 10.1109/ASEEZone1.2014.6820635.

[10] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, “Analysis of different text steganography techniques: A survey,” *Proc. - 2016 2nd Int. Conf. Comput. Intell. Commun. Technol. CICT 2016*, pp. 130–133, 2016, doi: 10.1109/CICT.2016.34.

[11] A. Singh and H. Singh, “An improved LSB based image steganography technique for RGB images,” *Proc. 2015 IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT 2015*, pp. 1–4, 2015, doi: 10.1109/ICECCT.2015.7226122.

[12] F. Akhter and M. Selim, “A New Approach of Graph Realization for Data Hiding using Human Encoding,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 12, 2016, doi: 10.14569/ijacsa.2016.071256.

[13] T. Anwar, S. Paul, and S. K. Singh, “Message transmission based on DNA cryptography: Review,” *Int. J. Bio-Science Bio-Technology*, vol. 6, no. 5, pp. 215–222, 2014, doi: 10.14257/ijbsbt.2014.6.5.22.

[14] M. Cui and Y. Zhang, “Incorporating Randomness into DNA Steganography to Realize Secondary Secret key, Self-destruction, and Quantum Key Distribution-like Function,” *bioRxiv*, p. 725499, 2019, [Online]. Available: http://biorxiv.org/content/early/2019/08/05/725499.abstract

[15] S. Alam, S. M. Zakariya, and M. Q. Rafiq, “Analysis of modified lsb approaches of hiding information in digital images,” *Proc. - 5th Int. Conf. Comput. Intell. Commun. Networks, CICN 2013*, pp. 280–285, 2013, doi: 10.1109/CICN.2013.66.

[16] A. K. Sahu and G. Swain, “A Novel n-Rightmost Bit Replacement Image Steganography Technique,” *3D Res.*, vol. 10, no. 1, 2019, doi: 10.1007/s13319-018-0211-x.

[17] M. M. Hashim, M. S. Mohd Rahim, and A. A. Alwan, “A review and open issues of multifarious image steganography techniques in spatial domain,” *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 4, pp. 956–977, 2018.

[18] S. Wendzel *et al.*, “A Revised Taxonomy of Steganography Embedding Patterns,” *ACM Int. Conf. Proceeding Ser.*, no. Ares, 2021, doi: 10.1145/3465481.3470069.

[19] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, “Hiding data in images using steganography techniques with compression algorithms,” *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.

[20] X. Huan, H. Zhou, and J. Zhong, “LSB based image steganography by using the fast marching method,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 1–5, 2019, doi: 10.14569/IJACSA.2019.0100301.

[21] I. Martmez, W. Fuertes, M. Palacios, D. Escudero, and T. Noboa, “RSA Over-Encryption Employing RGB Channels through a Steganography Variant,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 11, no. 4, pp. 1432–1439, 2021, doi: 10.18517/ijaseit.11.4.13728.

[22] S. Farrag and W. Alexan, “Secure 2D image steganography using recamán’s sequence,” *Proc. - 2019 Int. Conf. Adv. Commun. Technol. Networking, CommNet 2019*, pp. 1–6, 2019, doi: 10.1109/COMMNET.2019.8742368.

[23] M. Abdur, R. Ahmed, M. Adnan, and A. Ahmed, “Digital Image Security: Fusion of Encryption, Steganography and Watermarking,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 224–228, 2017, doi: 10.14569/ijacsa.2017.080528.

[24] M. M., A. A., and F. A., “An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 3, pp. 361–366, 2016, doi: 10.14569/ijacsa.2016.070350.

[25] J. Nath and A. Nath, “Advanced Steganography Algorithm using Encrypted secret message,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 3, 2011, doi: 10.14569/ijacsa.2011.020304.

[26] C. Paper and A. N. St, “Symmetric Key Cryptography Using Random Key Symmetric key cryptography using Random key generator,” no. November, 2015.

[27] A. Seif and W. Alexan, “A High Capacity Gray Code Based Security Scheme for Non-Redundant Data Embedding,” *Proc. 2020 Int. Conf. Innov. Trends Commun. Comput. Eng. ITCE 2020*, no. February, pp. 130–136, 2020, doi: 10.1109/ITCE48509.2020.9047755.

[28] N. Sakib, A. Hira, M. N. Mollah, S. M. Sharun, S. B. Mohamed, and M. A. Rashid, “SNR improvement and bandwidth optimization technique using PCM-DSSS encryption scheme,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 5, pp. 638–643, 2016, doi: 10.18517/ijaseit.6.5.921.

[29] D. T. Joy, G. Kaur, A. Chugh, and S. B. Bajaj, “Computer Vision for Color Detection,” *Int. J. Innov. Res. Comput. Sci. Technol.*, vol. 9, no. 3, pp. 53–59, 2021, doi: 10.21276/ijircst.2021.9.3.9.

[30] N. Phuangsaijai, J. Jakmunee, and S. Kittiwachana, “Investigation into the predictive performance of colorimetric sensor strips using RGB, CMYK, HSV, and CIELAB coupled with various data preprocessing methods: a case study on an analysis of water quality parameters,” *J. Anal. Sci. Technol.*, vol. 12, no. 1, 2021, doi: 10.1186/s40543-021-00271-9.

[31] U. Sara, M. Akter, and M. S. Uddin, “Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study,” *J. Comput. Commun.*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[32] J. Søgaard, L. Krasula, M. Shahid, D. Temel, K. Brunnström, and M. Razaak, “Applicability of existing objective metrics of perceptual quality for adaptive video streaming,” *IS T Int. Symp. Electron. Imaging Sci. Technol.*, 2016, doi: 10.2352/ISSN.2470-1173.2016.13.IQSP-206.

[33] R. Hassan, S. Kasim, W. A. Z. W. C. Jafery, and Z. A. Shah, “Image enhancement technique at different distance for Iris recognition,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 7, no. 4–2 Special Issue, pp. 1510–1515, 2017, doi: 10.18517/ijaseit.7.4-2.3392.

[34] B. R. Jana, H. Thotakura, A. Baliyan, M. Sankararao, R. G. Deshmukh, and S. R. Karanam, “Pixel density based trimmed median filter for removal of noise from surface image,” *Appl. Nanosci.*, no. 0123456789, 2021, doi: 10.1007/s13204-021-01950-0.

[35] M. Dalal and M. Juneja, “Steganography and Steganalysis (in digital forensics): a Cybersecurity guide,” *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, 2021, doi: 10.1007/s11042-020-09929-9.

[36] T. Bhuiyan, A. H. Sarower, M. Rashed Karim, and M. Maruf Hassan, “An image steganography algorithm using LSB replacement through XOR substitution,” *2019 Int. Conf. Inf. Commun. Technol. ICOIACT 2019*, pp. 44–49, 2019, doi: 10.1109/ICOIACT46704.2019.8938486.

[37] Scijs, “No Title,” *25 April*, 2017. https://github.com/scijs/baboon-image (accessed Aug. 17, 2022).

[38] Abejo, “No Title,” *free plane stock photos*. https://www.freeimages.com/photo/plane-1449679 (accessed Aug. 17, 2022).

[39] Irothko, “No Title.” https://www.freeimages.com/photo/singapore-mosque-1502213 (accessed Aug. 17, 2022).

[40] J. Peng *et al.*, “Implementation of the structural SIMilarity (SSIM) index as a quantitative evaluation tool for dose distribution error detection,” *Med. Phys.*, vol. 47, no. 4, pp. 1907–1919, 2020, doi: 10.1002/mp.14010.

[41] Z. A. Khan, T. Hussain, A. Ullah, S. Rho, M. Lee, and S. W. Baik, “Towards efficient electricity forecasting in residential and commercial buildings: A novel hybrid CNN with a LSTM-AE based framework,” *Sensors (Switzerland)*, vol. 20, no. 5, pp. 1–16, 2020, doi: 10.3390/s20051399.

[42] Q. A. Al-Haija and A. Ishtaiwi, “Machine Learning Based Model to Identify Firewall Decisions to Improve Cyber-Defense,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 11, no. 4, pp. 1688–1695, 2021, doi: 10.18517/ijaseit.11.4.14608.

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.