Jurnal Sifo Mikroskil (JSM)
Volume 27, No 1, April 2026 – Hal 73 - 92
DOI: https://doi.org/10.55601/jsm.v27i1.1866

e-ISSN: 2622-8130
ISSN: 1412-0100

Pengamanan Citra Warna Menggunakan Modified Reversible-Enhanced Stego Block Chaining dan Generator Modulo

David[1], Nicholas Ong[2], Ronsen Purba[3], Wulan Sri Lestari[4]
[1,2,3,4] Universitas Mikroskil, Jl. Thamrin No.124 Medan, (061) 4573767
[1,2,3,4] Fakultas Informatika, Teknik Informatika, Universitas Mikroskil, Medan
e-mail: [1]211110419@alumni.mikroskil.ac.id, [2]211110146@alumni.mikroskil.ac.id,
[3]ronsen@mikroskil.ac.id, [4]wulan.lestari@mikroskil.ac.id

Dikirim: ***14-08-2025*** | *Diterima:* ***20-04-2026*** | *Diterbitkan:* ***30-04-2026***

Abstrak

Keamanan komunikasi digital menjadi aspek yang semakin krusial seiring berkembangnya teknik analisis dan deteksi steganografi, sehingga diperlukan pendekatan penyisipan pesan yang lebih adaptif dan tidak mudah diprediksi. Penelitian ini mengusulkan metode *Modified Reversible-Enhanced Stego Block Chaining* (MRESBC) dengan dukungan Generator Modulo dan algoritma *Diffie-Hellman Key Exchange* (DHKE) untuk meningkatkan keamanan penyisipan pesan rahasia dalam citra warna. Metode ini memodifikasi teknik RESBC dengan menambahkan mekanisme pengacakan posisi sisip menggunakan generator modulo dan variasi bit penyisipan, serta menerapkan algoritma DHKE guna memperkuat pertukaran kunci secara aman dan sebagai seed awal dari generator modulo. Selain itu, data pesan dikompresi menggunakan algoritma *Lempel-Ziv-Welch* (LZW) guna mengoptimalkan kapasitas penyimpanan. Penelitian ini mengembangkan aplikasi prototipe dan pengujian dilakukan terhadap citra RGB 24-bit menggunakan metrik MSE, PSNR, dan SSIM. Hasil menunjukkan nilai PSNR terbaik sebesar 59,530 dB pada penyisipan 1-bit LSB dan terendah 36,583 dB pada 4-bit LSB dengan 3 stage, seluruhnya di atas ambang batas 30 dB. Nilai SSIM mencapai 1,0 pada seluruh skenario, mengindikasikan rekonstruksi citra pesan yang sempurna. Metode yang diusulkan terbukti mampu meningkatkan keamanan steganografi tanpa mengorbankan kualitas visual secara signifikan.

Kata kunci: Steganografi, RESBC, Generator Modulo, *Diffie-Hellman*, Citra Warna.

Abstract

Digital communication security has become increasingly crucial as steganalysis techniques continue to advance, necessitating more adaptive and unpredictable approaches to secret message embedding. This study proposes a method called Modified Reversible-Enhanced Stego Block Chaining (MRESBC), supported by a Modulo Generator and the Diffie-Hellman Key Exchange (DHKE) algorithm, to enhance the security of secret message embedding in color images. The method modifies the RESBC technique by adding a mechanism to randomize embedding positions using a modulo generator and by varying the number of embedded bits. Additionally, the DHKE algorithm is applied to securely perform key exchange and serve as the initial seed for the modulo generator. The secret message is also compressed using the Lempel-Ziv-Welch (LZW) algorithm to optimize storage capacity. In this research, a prototype application was developed and tested on 24-bit RGB images using MSE, PSNR, and SSIM metrics. Results show a best PSNR of 59.530 dB at 1-bit LSB embedding and a minimum of 36.583 dB at 4-bit LSB with 3 stages, all exceeding the 30 dB threshold. SSIM values reached 1.0 across all test scenarios, indicating perfect message reconstruction. The proposed method demonstrably enhances steganographic security without significantly compromising visual quality.

Keywords: *Steganography, RESBC, Modulo Generator, Diffie-Hellman, Color Image.*

1. PENDAHULUAN

Steganografi merupakan cara untuk menyembunyikan informasi atau data dalam bentuk apa pun (teks, gambar, suara, video) ke dalam media yang lebih besar (gambar, suara, video) sedemikian rupa sehingga tidak seorang pun mencurigai adanya keberadaan informasi atau data selain pengirim dan penerima [1]. Gambar merupakan salah satu media yang populer dan sering digunakan dalam steganografi [2]. Penelitian pada steganografi berfokus pada aspek penting seperti *imperceptibility, data payload, security, data integrity, robustness* dengan prioritas utama pada *imperceptibility* [3]. Penelitian dilakukan untuk meningkatkan *data payload* sambil tetap mempertahankan tingkat *imperceptibility* untuk mendapatkan kesimpulan lebih detail mengenai aspek *imperceptibility* dan *data payload*. Beberapa penelitian menggabungkan algoritma kompresi ke dalam teknik steganografi yang digunakan untuk menjaga tingkat *imperceptibility* dan meningkatkan *data payload*. Pengukuran tingkat kualitas *imperceptibility* diukur menggunakan metrik MSE (*Mean Squared Error*), PSNR (*Peak Signal-to-Noise Rasio)*, dan SSIM (*Structural Similarity Indeks)* [3,4,5]

Beberapa penelitian telah dilakukan untuk mengatasi kelemahan dari teknik LSB, seperti penelitian [6] yang mengusulkan dua modifikasi dari teknik LSB yaitu *Bit Inverse* dan penyisipan berdasarkan panjang pesan. Modifikasi *Bit Inverse* mendapatkan hasil yang cukup baik dengan nilai PSNR = 61.80 dB untuk pesan teks dengan 2110 karakter dan PSNR = 50.01 dB untuk gambar, modifikasi ini memiliki kelemahan yaitu kualitas gambar menurun pada daerah tertentu karena penyisipan beruntun sehingga berisiko untuk dikenali. Sebaliknya, modifikasi penyisipan berdasarkan panjang pesan menunjukkan hasil PSNR yang lebih tinggi dibandingkan dengan modifikasi *Bit Inverse* dengan PSNR = 66.29 dB untuk pesan teks dan PSNR = 54.20 dB untuk gambar. Kemudian pada penelitian [7] yang menggunakan teknik 2 LSB, yang merupakan variasi dari teknik LSB di mana jumlah bit yang disisipkan sebanyak 2 bit sehingga meningkatkan kapasitas dari teknik LSB. Hasil penelitian ini dievaluasi menggunakan metrik MSE dan PSNR, dan mendapatkan nilai masing-masing 0.0012 dan 49.65 dB untuk gambar dengan ukuran 1024 x 1024 *pixel*. Namun, teknik 2 LSB memiliki kelemahan di mana penyisipan pada 2 bit terakhir dapat meningkatkan risiko distorsi visual pada gambar dengan kualitas rendah ataupun gambar dengan banyak variasi warna sehingga membuat pemilihan gambar menjadi cukup penting agar teknik ini mendapatkan performa yang optimal.

Selanjutnya, penelitian [8] menggunakan konsep *Reversible-Enhanced Stego Block Chaining* (RESBC). Konsep ini mendapatkan hasil yang baik dengan *Hiding Capacity* (HC) hingga 73.74% dengan nilai PSNR sebesar 38.75 dB untuk penyisipan sebanyak 3 *stage* dengan menggunakan algoritma kompresi HE-SFA-LZW pada tiap *stage*. Meskipun konsep ini memiliki hasil yang baik dan lebih aman dibandingkan dengan teknik 4 LSB, namun keamanan metode ini dapat ditingkatkan dengan melakukan pengacakan karena penyisipan masih dilakukan secara berurutan. Lebih lanjut, pada penelitian [9] menggabungkan *Simulated Annealing* (SA), *Linear Congruential Generator* (LCG), dan *Caesar Cipher* dengan teknik LSB dan mendapatkan hasil yang cukup baik dengan nilai PSNR hingga 68.36 dB untuk pesan sebesar 1868 *bytes* dan citra sampul berukuran 768432 *bytes,* namun metode ini memiliki kelemahan di mana LCG memiliki siklus terbatas, mudah diprediksi serta rentan terhadap serangan *brute force*.

Teknik LSB dipilih karena merupakan teknik yang paling mudah untuk diterapkan [3], namun teknik LSB memiliki kelemahan karena kapasitas yang kecil dan penyisipan dilakukan secara berurutan sehingga rentan terdeteksi pada area piksel yang berdekatan [3,6]. Untuk lebih meningkatkan ketahanan sistem terhadap analisis steganalisis, diperlukan mekanisme pemilihan posisi piksel yang tidak berpola, sehingga digunakan *Pseudo-Random Number Generator* (PRNG) yang menghasilkan urutan bilangan berdasarkan aturan algoritma tertentu sehingga terlihat acak namun bersifat deterministik [10]. Salah satu implementasinya adalah LCG, yang bekerja berdasarkan nilai seed awal yang ditetapkan oleh pengguna serta harus memenuhi sejumlah prasyarat matematis untuk menghasilkan urutan bilangan tanpa pengulangan [9]. Karena sifat deterministik tersebut, urutan bilangan yang dihasilkan dapat

direproduksi apabila parameter awal diketahui, sehingga penggunaan dan pengelolaan nilai seed menjadi aspek penting dalam menjaga keamanan sistem. Oleh karena itu, penelitian ini mengusulkan penerapan algoritma *Diffie-Hellman* sebagai mekanisme pertukaran kunci untuk meningkatkan keamanan distribusi nilai seed terhadap pihak yang tidak berwenang.

Kontribusi ilmiah penelitian ini terletak pada dua aspek utama yang membedakannya dari metode RESBC [8]: (1) penerapan mekanisme pengacakan posisi penyisipan berbasis Generator Modulo yang menggantikan terhadap pola penyisipan berurutan, sehingga mengurangi risiko terdeteksi; serta (2) integrasi algoritma *Diffie-Hellman Key Exchange* (DHKE) sebagai seed generator modulo, yang memastikan nilai awal kunci bersifat rahasia dan tidak deterministik sehingga meningkatkan keamanan. Berbeda dengan RESBC orisinal yang menggabungkan beberapa algoritma kompresi berbeda pada tiap *staging*, penelitian ini secara konsisten menggunakan algoritma kompresi LZW pada seluruh *staging*. Keputusan ini didasarkan pada hasil yang dilaporkan dalam penelitian, di mana kompresi LZW cenderung menghasilkan tingkat kompresi lebih tinggi [11], atau nilai kapasitas penyisipan dan PSNR yang lebih tinggi dibandingkan metode kompresi lainnya [8].

2. TINJAUAN PUSTAKA

2.1 LSB (Least Significant Bit)

Least Significant Bit adalah salah satu teknik steganografi paling populer dan sederhana yang digunakan untuk menyembunyikan pesan rahasia dalam citra digital. Metode ini bekerja dengan menyisipkan bit pesan rahasia ke dalam bit paling tidak signifikan dari setiap *pixel* pada gambar. Bit pesan rahasia diubah ke dalam bentuk biner dan kemudian didistribusikan di antara LSB dari setiap *pixel*. Karena perubahan ini terjadi pada bit terkecil, dampaknya pada kualitas visual gambar sangat minim, sehingga pesan tersembunyi sulit untuk dideteksi [12,13,14,15].

Metode ini mudah dilakukan, karena bit pesan rahasia langsung dimasukkan ke dalam bit yang memiliki nilai paling rendah pada gambar. Namun, karena penyisipan dilakukan secara berurutan dari bit yang paling kanan, pesan menjadi mudah diekstraksi jika seseorang mencurigai adanya informasi rahasia dalam gambar. Kemudahan ekstraksi ini merupakan salah satu kelemahan dari teknik LSB [16].

2.2 RESBC (Reversible-Enhanced Stego Block Chaining)

RESBC merupakan teknik steganografi berbasis blok yang dikembangkan untuk meningkatkan kapasitas dan keamanan pesan tanpa mengorbankan kualitas visual dari citra digital. RESBC bekerja dengan membagi citra sampul menjadi beberapa blok-blok kecil yang kemudian akan digunakan sebagai media penyisipan pesan rahasia, setiap blok menjalani proses penyisipan secara berantai (*chaining*) melalui beberapa tahapan yang disebut *staging*.

RESBC memiliki sifat *reversible* yang memungkinkan *stego-image* dikembalikan ke bentuk awalnya secara utuh setelah pesan rahasia diekstraksi. Hal ini dapat dicapai dengan memanfaatkan algoritma *chaining* antarblok, di mana proses penyisipan satu blok akan memengaruhi penyisipan pada blok berikutnya [8].

2.3 DHKE (Diffie-Hellman Key Exchange)

Diffie-Hellman Key Exchange adalah algoritma pertukaran kunci asimetris yang memungkinkan dua pihak untuk berbagi kunci rahasia melalui saluran komunikasi yang tidak aman tanpa harus berbagi kunci sebelumnya [17,18]. Pertukaran kunci ini didasarkan pada kesulitan dalam menghitung logaritma diskrit, yaitu sebuah permasalahan matematika yang juga menjadi dasar keamanan pada algoritma El Gamal. Nilai kunci yang dihasilkan bergantung kepada para peserta dan informasi mengenai kunci publik dan privat mereka masing-masing [19].

Prinsip kerja DHKE antara lain [17,18]:

1. Alice dan Bob sepakat dua parameter publik
   - p: bilangan prima besar.

- g: bilangan yang disebut generator modulo p.

2. Alice dan Bob memilih kunci privat secara acak
   - Alice memilih a
   - Bob memilih b
3. Masing-masing menghitung kunci publik
   - Alice menghitung $A = g^a \ mod \ p$ dan mengirimkan A kepada Bob.
   - Bob menghitung $B = g^b \ mod \ p$ dan mengirimkan B kepada Alice.
4. Keduanya menghitung kunci rahasia bersama K
   - Alice: $K = \ B^a \ mod \ p$
   - Bob: : $K = \ A^b \ mod \ p$
   - Karena sifat aritmetika modular, hasilnya sama dengan $K = g^{(a+b)} \ mod \ p$

2.4 Generator Modulo

Generator modulo digunakan untuk menghasilkan urutan angka acak yang menentukan posisi piksel pada *cover image* tempat bit pesan rahasia akan disisipkan. Jenis generator modulo yang digunakan yaitu *Fast Exponensial*. *Fast Exponential* digunakan untuk melakukan operasi pemangkatan dengan cepat pada bilangan bulat modulo. Dalam metode ini, ekspansi biner dari eksponen dimanfaatkan. Misalkan kita memiliki himpunan G, dan $g \in G$, sedangkan z adalah bilangan bulat positif. Untuk menghitung g^z menggunakan metode *fast exponentiation*, langkah-langkahnya adalah sebagai berikut:

a. Hitung $g^{2^i}, 0 \leq 1 < k$.
b. Nilai g^z adalah hasil perkalian dari nilai-nilai g^{2^i}, dengan $a_1 = 1$. Diperoleh persamaan (1):

$$g^{2^{i+1}} = \left(g^{2^i}\right)^2 \quad (1)$$

Penelitian [20] menuliskan jika p adalah bilangan prima, maka himpunan bilangan $\{1,2, \dots, p-1\}$ membentuk perkalian modulo p, yang disebut $(\frac{\mathbb{Z}}{p\mathbb{Z}})$. Akar primitif dari p adalah bilangan $g \in (\frac{\mathbb{Z}}{p\mathbb{Z}})$ yang dapat menghasilkan semua elemen grup melalui perpangkatan atau dengan kata lain g adalah generator dari $(\frac{\mathbb{Z}}{p\mathbb{Z}})$ seperti yang dapat dilihat pada persamaan (2) berikut:

$$\{g^1 \ mod \ p, g^2 \ mod \ p, \dots, g^{p-1} \ mod \ p\} = \{1, 2, \dots, p-1\} \quad (2)$$

Untuk mencari akar primitif dari bilangan prima, digunakan pendekatan berbasis teori ordo dan Teorema Kecil Fermat. Langkahnya adalah sebagai berikut:

1. Menghitung nilai dari $p - 1$.
2. Memfaktorkan bilangan $p - 1$ menjadi faktor prima seperti yang dapat dilihat pada persamaan (3)

$$p - 1 = q_1^{k_1} \cdot q_2^{k_2{}'} \cdot \cdots \cdot q_n^{k_n} \quad (3)$$

Di mana:

1) $p - 1$ merupakan jumlah elemen dalam grup perkalian modulo p, yaitu $(\frac{\mathbb{Z}}{p\mathbb{Z}})$.
2) $q_1, q_2, \dots, q_n$ merupakan faktor-faktor prima dari $p - 1$.
3) $k_1, k_2, \dots, k_n$ merupakan pangkat dari masing-masing faktor prima, jadi $q_i^{k_i}$ menunjukkan bahwa q_i muncul sebanyak k_i kali dalam faktorisasi.

3. Uji semua nilai g dari 2 hingga $p - 1$. Untuk setiap g seperti pada persamaan (4) berikut:

$$g^{\frac{(p-1)}{q_i}} \ mod \ p \ \neq 1 \text{ untuk semua } q_i \quad (4)$$

Jika semua hasil tidak sama dengan 1, maka g adalah akar primitif dari p.

2.5 Metrik Pengujian

Evaluasi terhadap metode yang telah diterapkan perlu dilakukan, evaluasi ini dapat dilakukan dengan menggunakan beberapa metrik pengukuran seperti [21]:

1. MSE (*Mean Squared Error*), mengukur rata-rata selisih kuadrat antara piksel citra asli dan hasil steganografi untuk menilai tingkat distorsi, di mana nilai MSE yang lebih rendah menunjukkan distorsi visual yang lebih kecil. MSE dapat dihitung dengan rumus:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(x_{i,j} - x'_{i,j}\right)^2 \quad (5)$$

   Di mana:
   1) $x_{i,j}$ adalah nilai *pixel* pada gambar asli.
   2) $x'_{i,j}$ adalah nilai *pixel* pada *stego-image*.
   3) M dan N adalah ukuran gambar (jumlah baris dan kolom).
2. PSNR (*Peak Signal-to-Noise Ratio*), unakan untuk mengukur kualitas citra steganografi dengan membandingkan sinyal puncak terhadap bunyi, di mana nilai PSNR yang lebih tinggi menunjukkan kesetiaan visual citra yang lebih baik terhadap citra asli. PSNR dapat dihitung menggunakan rumus:

$$PSNR = 10\, log_{10} \left(\frac{255^2}{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(x_{i,j} - x\prime_{i,j}\right)^2} \right) \quad (6)$$

   Di mana:
   1) 255 adalah nilai maksimum *pixel* dalam citra 8 bit (0-255)
   2) $x_{i,j}$ adalah nilai *pixel* pada gambar asli.
   3) $x'_{i,j}$ adalah nilai *pixel* pada *stego-image*.
   4) M dan N adalah ukuran gambar (jumlah baris dan kolom).
3. SSIM (*Structural Similarity Index)*, digunakan untuk mengukur tingkat kemiripan antara dua gambar berdasarkan pencahayaan, kontras dan struktur. SSIM dapat dihitung menggunakan rumus:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C1)(2\sigma_{xy} + C2)}{(\mu_x^2 + \mu_y^2 + C1)(\sigma_x^2 + \sigma_y^2 + C2)} \quad (7)$$

   Di mana:
   1) μ_x, μ_y merupakan nilai rata-rata intensitas *pixel* dari citra x dan y, serta mewakili komponen kecerahan dari masing-masing citra.
   2) σ_x^2, σ_y^2 merupakan varians dari citra x dan y yang menunjukkan kontras dari masing-masing citra.
   3) $\sigma_{x,y}$ merupakan kovarians antara citra x dan y yang merepresentasikan kesamaan pola antara dua citra.
   4) C_1, C_2 merupakan konstanta kecil yang digunakan untuk mencegah pembagian dengan nol. Biasanya didefinisikan oleh persamaan (8)

$$C_1 = (K_1 L)^2, C_2 = (K_2 L)^2 \quad (8)$$

      Di mana:
      1) L merupakan rentang dinamis *pixel* (misalnya 255 untuk gambar 8-bit)
      2) $K_1 \approx 0.01, K_2 \approx 0.03$

3. METODE PENELITIAN

3.1 Tahapan Penelitian

Penelitian ini menggunakan pendekatan sistematis untuk mengembangkan metode steganografi berbasis *Modified Reversible-Enhanced Stego Block Chaining* (MRESBC) yang diintegrasikan dengan Generator Modulo dan algoritma *Diffie-Hellman Key Exchange* (DHKE). Tahapan penelitian yang dilakukan meliputi:

1. Studi Literatur dan Analisis Metode

Pada tahap ini dilakukan pembelajaran mendalam terhadap referensi yang berkaitan dengan teknik RESBC, generator modulo, proses DHKE, dan teknik steganografi LSB. Analisis dilakukan

terhadap kelemahan metode yang telah ada dan melakukan identifikasi bagian yang dapat diperbaiki untuk mengembangkan metode yang lebih aman.

2. Persiapan Data Penelitian

Tahap ini bertujuan untuk mengumpulkan dan mempersiapkan citra sampul dan citra pesan yang digunakan dalam penelitian. Citra yang digunakan bersumber dari USC-SIPI (*University of Southern California - Signal and Image Processing Institute*) *Image Database*, khususnya koleksi *miscellaneous*. Setelah citra dikumpulkan, dilakukan *preprocessing* data yang terdiri dari:

a. Konversi Format Citra
   Konversi format citra yang awalnya berformat TIFF dikonversi ke format BMP menggunakan bahasa pemrograman Python dengan *library* PIL (*Python Imaging Library*). Citra *grayscale* dikonversi menjadi 8-bit BMP, sedangkan citra berwarna dikonversi menjadi 24-bit RGB BMP.
b. *Resize* Citra
   Semua citra di-*resize* menjadi ukuran persegi menggunakan metode *crop* dari tengah dan *scaling* dengan algoritma LANCZOS *resampling* untuk mempertahankan kualitas citra. Penyeragaman ukuran ini diperlukan untuk memastikan konsistensi dalam proses penyisipan dan ekstraksi, serta memudahkan analisis perbandingan hasil.

3. Perancangan Metode MRESBC

Dilakukan perancangan metode yang mengintegrasikan modifikasi RESBC dengan generator modulo dan DHKE. Perancangan mencakup alur proses penyisipan dan ekstraksi yang detail, termasuk mekanisme pengacakan posisi sisip, pembentukan kunci keamanan, dan implementasi kompresi LZW.

Metode yang diusulkan memodifikasi teknik RESBC dengan menambahkan mekanisme pengacakan posisi sisip menggunakan generator modulo dan variasi bit penyisipan, serta menerapkan algoritma DHKE untuk memperkuat keamanan. Arsitektur sistem terdiri dari empat komponen utama yang saling terintegrasi: algoritma *Diffie-Hellman Key Exchange* untuk pembentukan kunci rahasia, Generator Modulo untuk pengacakan posisi penyisipan, algoritma *Lempel-Ziv-Welch* untuk kompresi data, dan *Modified Reversible-Enhanced Stego Block Chaining* sebagai mekanisme penyisipan bertingkat.

4. Implementasi dan Validasi Metode

Implementasi metode MRESBC dilakukan untuk memvalidasi konsep yang telah dirancang. Sistem dibangun untuk memproses citra pesan (RGB 24-bit atau *Grayscale* 8-bit) dan citra sampul (RGB 24-bit) dengan parameter input berupa kunci pribadi (Xa, Xb), jumlah *staging* (1-3), dan jumlah bit sisip (1-4). Output yang dihasilkan berupa *stego-image* pada proses penyisipan dan citra pesan hasil ekstraksi pada proses ekstraksi.

5. Pengujian dan Evaluasi

Pengujian dilakukan menggunakan tiga metrik evaluasi utama. Tingkat *imperceptibility* diukur menggunakan MSE dan PSNR dengan membandingkan citra sampul asli dan *stego-image* yang dihasilkan. Kualitas *recovery* pesan dievaluasi menggunakan SSIM untuk memverifikasi bahwa pesan tersembunyi dapat diekstraksi dengan sempurna tanpa kehilangan data. Selain itu, dilakukan pengujian terhadap kunci DHKE yang dihasilkan berdasarkan variasi parameter untuk memvalidasi konsistensi dan keamanan sistem. Pengujian menggunakan citra RGB 24-bit dengan variasi jumlah bit sisip (1-4) dan jumlah *stage* (1-3).

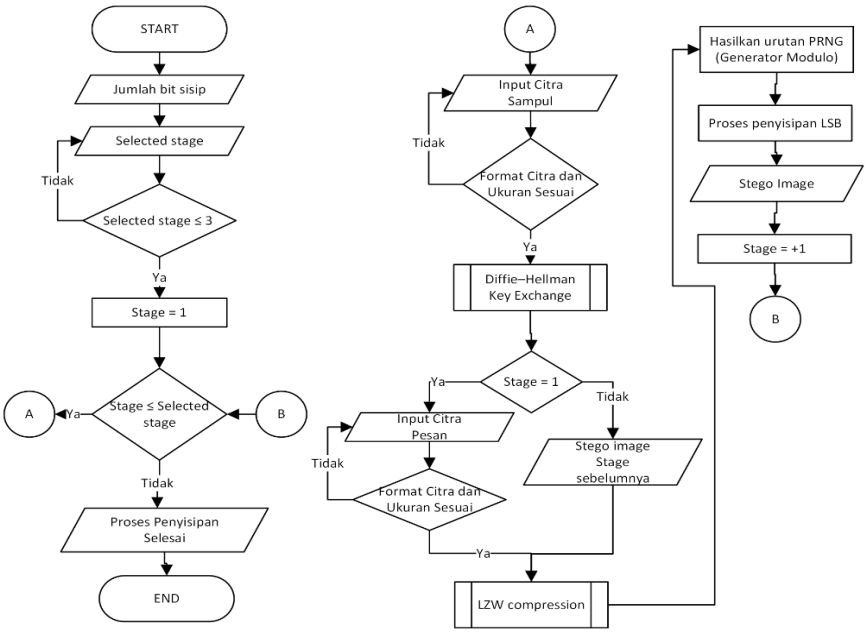
Validasi ketahanan terhadap serangan steganalisis, belum dilakukan dalam lingkup penelitian ini dan menjadi rekomendasi untuk penelitian lanjutan. Meskipun demikian, mekanisme pengacakan posisi penyisipan berbasis Generator Modulo yang dikombinasikan dengan seed DHKE secara teoritis mempersulit deteksi melalui analisis distribusi statistik piksel karena posisi penyisipan tidak membentuk pola berurutan yang dapat diidentifikasi

6. Analisis Hasil dan Penarikan Kesimpulan

Penarikan kesimpulan dilakukan setelah seluruh tahap pengujian terhadap sistem selesai dilaksanakan. Evaluasi dilakukan terhadap pencapaian tujuan penelitian, analisis hasil pengujian berdasarkan metrik yang telah ditetapkan, identifikasi kelebihan sistem yang telah dibangun, serta rekomendasi untuk pengembangan lebih lanjut.

3.2 Proses Penyisipan dengan Modified RESBC

Proses penyisipan pesan dilakukan melalui beberapa tahapan berurutan yang dimulai dari input parameter hingga menghasilkan *stego-image*. Tahapan ini meliputi penentuan jumlah bit sisip, *selected stage*, dan pembentukan *Diffie-Hellman Key Exchange*, dilanjutkan dengan kompresi LZW, menghasilkan urutan PRNG menggunakan generator modulo, dan proses penyisipan LSB dengan posisi acak. Modifikasi utama dari metode RESBC terletak pada penambahan mekanisme pengacakan posisi penyisipan yang memanfaatkan generator modulo berbasis DHKE, sehingga tidak lagi menggunakan pola penyisipan berurutan yang rentan terhadap deteksi. Selain itu, implementasi kompresi LZW sebelum proses penyisipan memungkinkan optimalisasi kapasitas penyimpanan data rahasia. Proses penyisipan secara keseluruhan dapat dilihat pada Gambar 1.



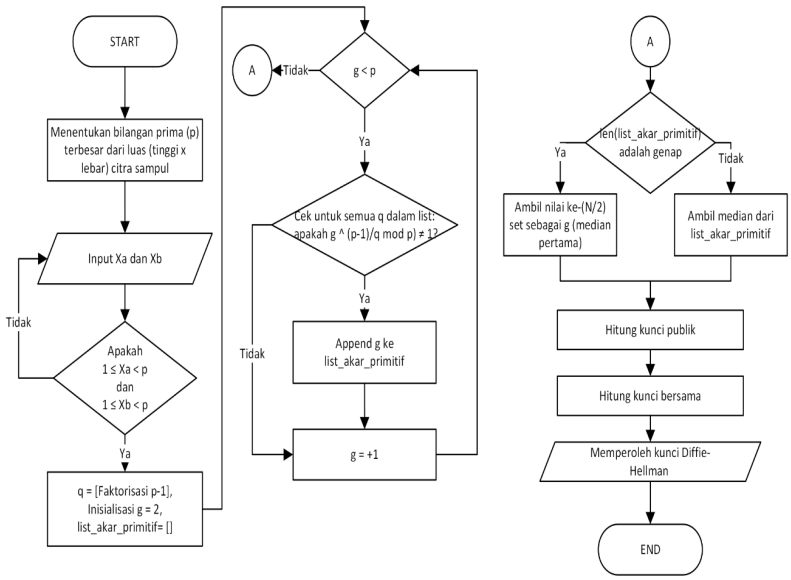
Gambar 1. *Flowchart* Proses Penyisipan

Pada tahap awal, sistem menerima input berupa jumlah bit sisip yang merupakan jumlah bit yang akan disisipkan per *channel* ke dalam citra sampul dengan rentang 1-4 bit. *Selected stage* merupakan input jumlah *stage* yang akan diproses dengan maksimal 3 *stage*. *Stage* dimulai dari *index* 1 dan dilakukan pengecekan apakah *stage* sudah selesai sesuai dengan input yang ditentukan. Untuk setiap *stage*, diperlukan input citra sampul baru untuk menyesuaikan ukuran pesan hasil kompresi LZW.

3.2.1 Pembentukan Diffie-Hellman Key Exchange

Proses pembentukan DHKE dimulai dengan menentukan bilangan prima terbesar dari luas (tinggi × lebar) citra sampul. Input Xa dan Xb merupakan kunci privat yang digunakan untuk menghasilkan kunci *Diffie-Hellman* yang sama. Nilai Xa dan Xb memiliki persyaratan $1 \leq Xa < p$ dan $1 \leq Xb < p$, jika tidak memenuhi maka akan dilakukan input ulang. Proses pembentukan DHKE untuk penyisipan dapat dilihat pada Gambar 2.

2622-8130 Jurnal Sifo Mikroskil (JSM) - Volume 27, No 1, April 2026
DOI: https://doi.org/10.55601/jsm.v27i1.1866



Gambar 2. *Flowchart* Proses Pembentukan DHKE Untuk Penyisipan

Sistem menghitung faktorisasi p-1 dan menyimpannya ke dalam *list* q, menginisialisasi g = 2 sebagai awalan mencari kemungkinan nilai akar primitif dari prima (g), dan menginisialisasikan *list_akar_primitif* untuk menyimpan nilai g yang valid. Semua kemungkinan nilai g dalam rentang $2 \leq g \leq p-1$ yang memiliki hasil $\neq 1$ akan dimasukkan ke dalam *list_akar_primitif*.

Sebagai contoh, jika citra sampul berukuran 7×7 *pixel*, maka bilangan prima terbesarnya adalah 47. Proses menentukan generator mengikuti aturan *Diffie-Hellman* dengan p = 47, p-1 = 46, dan faktorisasi p-1 = 2 × 23. Sistem menguji semua kemungkinan g dalam rentang $2 \leq g \leq p-1$ dengan kondisi $(g^{((p-1)/2)}) \bmod p \neq 1$ dan $(g^{((p-1)/23)}) \bmod p \neq 1$. Berdasarkan hasil perhitungan, diperoleh *list_akar_primitif* dengan beberapa akar primitif yaitu 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, dan 45. Median dari akar primitif tersebut adalah 29 dan 30, dan sistem memilih angka pertama yaitu 29 sebagai generator.

Setelah generator ditentukan, sistem menghitung kunci publik menggunakan:

$$Ya = g^{Xa} \bmod p \quad (9)$$

$$Yb = g^{Xb} \bmod p \quad (10)$$

Dengan contoh Xa = 4 dan Xb = 3, diperoleh $Ya = 29^4 \bmod 47 = 25$ dan $Yb = 29^3 \bmod 47 = 43$. Kunci bersama (*shared key*) dihitung menggunakan:

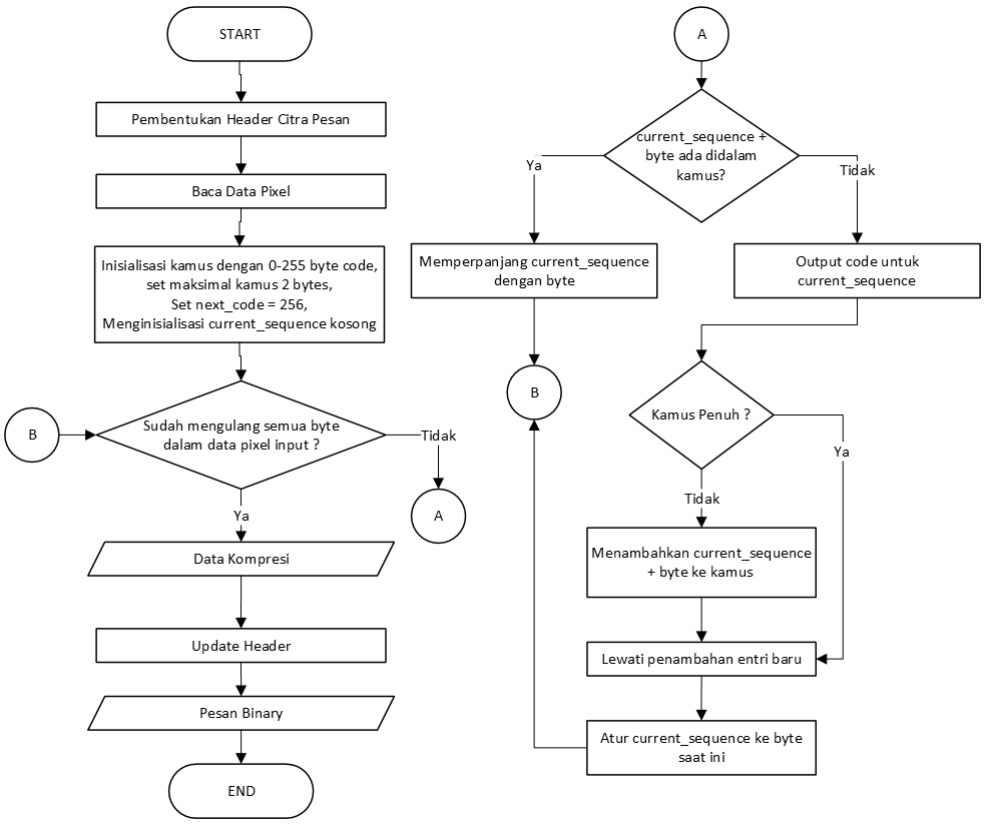
$$K = Yb^{Xa} \bmod p = Ya^{Xb} \bmod p \quad (11)$$

Hasil kunci *Diffie-Hellman* yang diperoleh adalah K = 21.

3.2.2 Kompresi LZW dan Generator Modulo

Pada *stage* = 1, pesan merupakan input citra pesan. Jika *stage* = 2, pesan akan menggunakan *stego-image* hasil proses dari *stage* 1, dan jika *stage* = 3, pesan akan menggunakan *stego-image* hasil proses dari *stage* 2. Proses LZW *compression* dapat dilihat pada Gambar 3.

2622-8130 Jurnal Sifo Mikroskil (JSM) - Volume 27, No 1, April 2026
DOI: https://doi.org/10.55601/jsm.v27i1.1866



Gambar 3. *Flowchart* Proses LZW *Compression*

Pembentukan *header* citra pesan dilakukan dengan membaca informasi pada citra pesan mengenai jumlah *channel* (1 *byte*), tinggi (2 *bytes*), lebar (2 *bytes*) dan *Diffie-Hellman key* (4 *bytes*). Data *pixel* citra pesan dikonversi menjadi bilangan desimal pada setiap *pixel* dengan urutan pembacaan secara raster scan. Untuk citra RGB, konversi dilakukan berdasarkan channel secara berurutan: dimulai dari *channel* R yang dibaca dari baris pertama kiri ke kanan hingga baris terakhir, kemudian dilanjutkan dengan *channel* G dengan pola pembacaan yang sama, dan terakhir *channel* B. Sedangkan untuk citra *grayscale*, konversi dilakukan sekali dengan pola pembacaan raster scan dari kiri ke kanan dan atas ke bawah tanpa pemisahan *channel*. Kamus diinisialisasi dengan nilai *byte* tunggal (0-255), *next_code* diset dengan nilai 256, dan maksimal kamus 2 *bytes* (65535 dalam desimal). Setelah data kompresi didapatkan dilakukan *update header* dengan menambahkan informasi total *byte* hasil kompresi (4 *bytes*).

Sistem menghasilkan urutan PRNG (*Pseudo Random Number Generator*) menggunakan generator modulo untuk pengacakan posisi sisip pesan terhadap citra sampul. Total posisi *pixel* yang dibutuhkan dihitung menggunakan:

$$\text{Total Posisi } Pixel \text{ LSB} = \left\lceil \frac{\text{Total } byte \text{ pesan} \times 8 \text{ bit}}{\text{LSB} \times 3 \text{ } Channel \text{ RGB}} \right\rceil \quad (12)$$

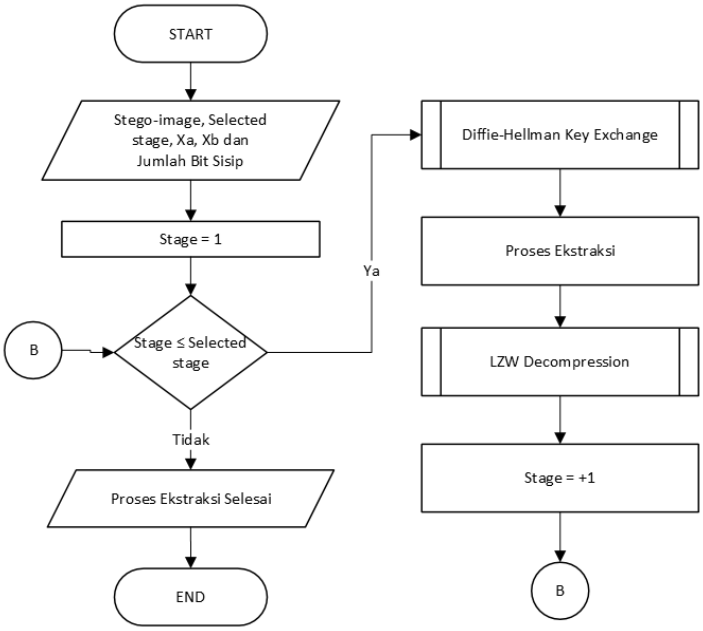
Dengan kunci *Diffie-Hellman* sebagai nilai awal, sistem menghasilkan PRNG menggunakan:

$$\text{PRNG (Generator Modulo)} = g^n \bmod p \quad (13)$$

dimana n dimulai dari angka *DH key* sebagai iterasi pertama dan iterasi selanjutnya bertambah 1. Jika nilai n ≥ p, maka iterasi dimulai dengan n menjadi 1.

3.3 Proses Ekstraksi dengan Modified RESBC

Proses ekstraksi dilakukan untuk mengambil kembali pesan rahasia dari *stego-image* melalui tahapan validasi *Diffie-Hellman Key Exchange*, ekstraksi pesan *staging*, dan LZW *decompression*. Proses ekstraksi secara keseluruhan dapat dilihat pada Gambar 4.

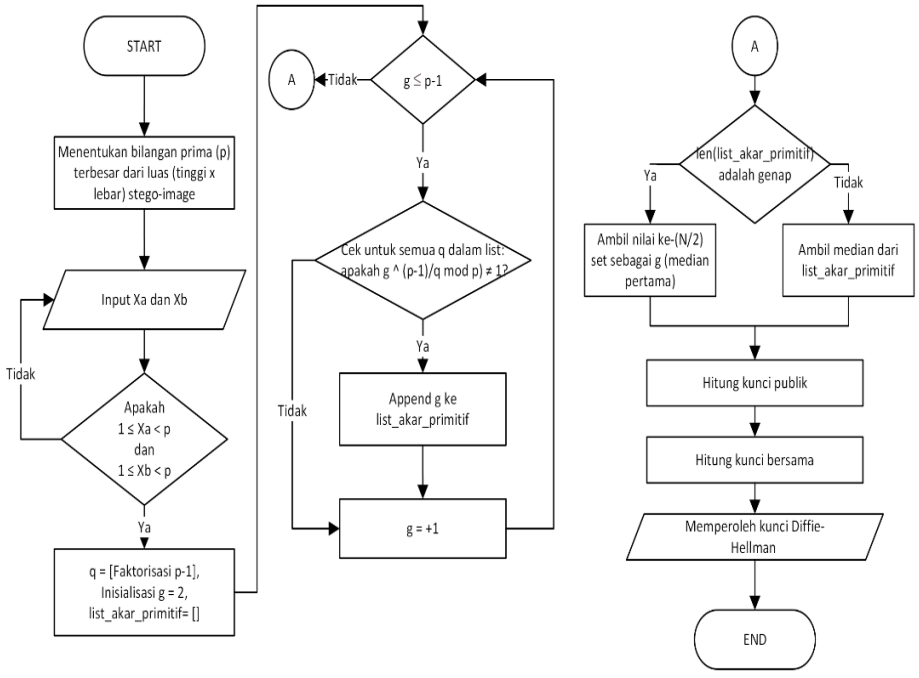


Gambar 4. *Flowchart* Proses Ekstraksi

Tahapan ekstraksi dimulai dengan mengubah *stego-image* ke dalam format biner, menghitung nilai *Diffie-Hellman Key Exchange* untuk validasi, melakukan proses ekstraksi bit, dan LZW *decompression* untuk rekonstruksi citra pesan.

3.3.1 Pembentukan Diffie-Hellman Key Exchange

Proses pembentukan DHKE untuk ekstraksi dapat dilihat pada Gambar 5.



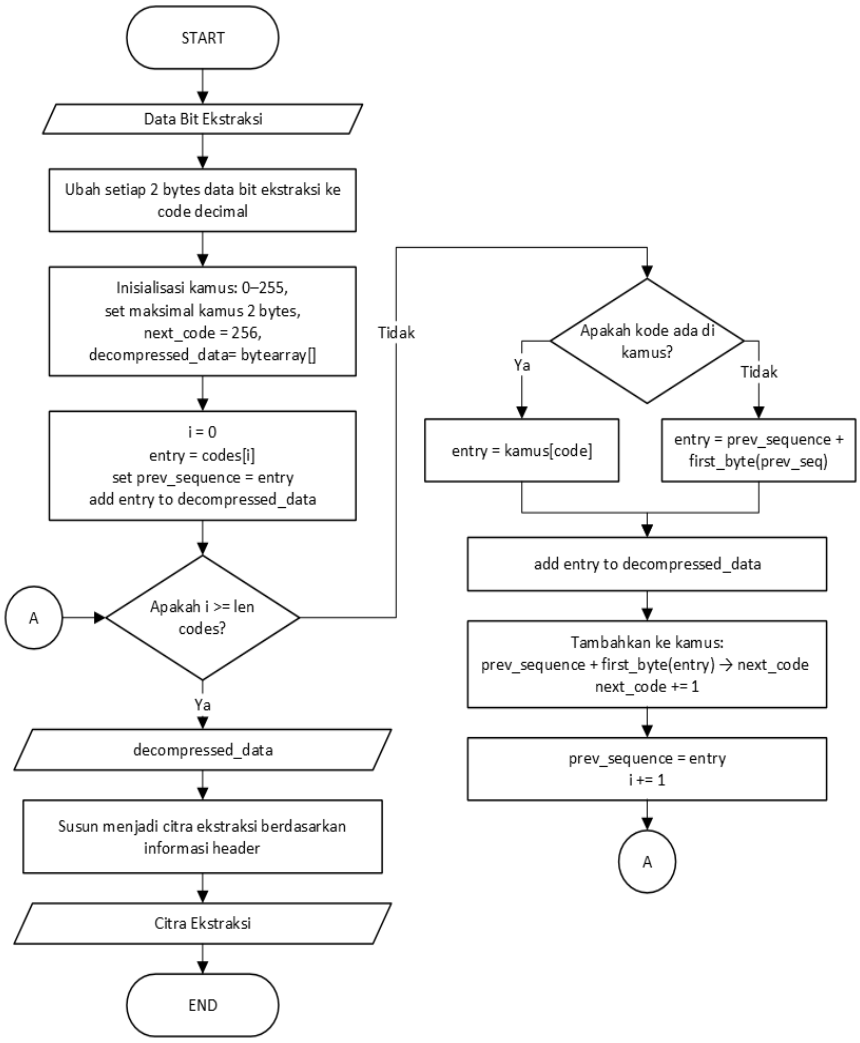
Gambar 5. *Flowchart* Proses Pembentukan DHKE Untuk Ekstraksi

Sistem menentukan bilangan prima terbesar dari luas (tinggi × lebar) *stego-image* dan menerima input Xa dan Xb yang harus sama dengan nilai yang digunakan saat penyisipan. Sistem mencari nilai g dalam rentang $2 \leq g \leq p-1$ yang menghasilkan nilai $\neq 1$, menentukan nilai median dari *list_akar_primitif*, menghitung kunci publik, dan menghitung kunci bersama. Kunci *Diffie-Hellman* yang dihasilkan selanjutnya digunakan untuk proses validasi *header.*

3.3.2 Ekstraksi Data dan Rekonstruksi Citra

Setelah mendapatkan kunci *Diffie-Hellman* dilakukan ekstraksi dengan menggunakan generator modulo yang sama dengan proses penyisipan di mana kunci *Diffie-Hellman* yang telah dihasilkan menjadi iterasi pertama. Ekstraksi dimulai dengan mengambil 13 *bytes* pertama untuk informasi *header* menggunakan posisi yang dihasilkan oleh PRNG. Proses validasi dilakukan dengan mencocokkan kunci DHKE yang dihitung dengan kunci referensi dalam *header*. Ekstraksi data pesan menggunakan urutan posisi yang dibangkitkan oleh generator modulo. Untuk setiap posisi *pixel* yang ditentukan oleh PRNG, sistem mengekstraksi LSB dari *channel* R, G, dan B secara berurutan hingga mencapai total bit yang sesuai dengan ukuran data terkompresi dalam *header.*

Proses LZW *decompression* dapat dilihat pada Gambar 6.



Gambar 6. *Flowchart* Proses LZW *Decompression*

Setelah mendapatkan pesan data ekstraksi yang benar berdasarkan informasi *header*, data ekstraksi dikonversi setiap 2 *bytes* ke dalam kode bilangan desimal dan diproses menggunakan *dekompresi* LZW. Kamus diinisialisasi dengan karakter dasar ASCII, dan setiap kode input diproses untuk menghasilkan output yang sesuai.

Hasil output dekompresi berupa *stream byte* yang kemudian dikonversi ke format bit dan disusun kembali menjadi citra pesan berdasarkan informasi *header* (jumlah *channel*, tinggi, lebar). Untuk proses *multi-staging*, citra hasil ekstraksi akan menjadi *stego-image* untuk *stage* berikutnya hingga mendapatkan citra pesan asli.

4. HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan dilakukan pengujian pembentukan *Diffie-Hellman Key Exchange* (DHKE), uji MSE dan PSNR pada *stego-image*, lalu pengujian uji SSIM pada citra pesan ekstraksi dengan citra pesan *original*.

4.1 Pembentukan Diffie-Hellman Key Exchange (DHKE)

Citra pesan dan sampul yang digunakan untuk menjelaskan pembentukan DHKE dapat dilihat pada Gambar 7.

a b c

Gambar 7. (a) Jelly beans, (b) Female 2, (c) Female

Hasil pengujian pengaruh nilai parameter inputan terhadap pembentukan DHKE dapat dilihat pada Tabel 1.

Tabel 1. Hasil Pembentukan DHKE Terhadap Parameter Dengan Citra Pesan Jelly beans

No. Uji	Dimensi Citra Pesan	Citra Sampul *Staging* 1	Dimensi Citra Sampul *Staging* 1	Xa	Xb	p	g	Ya	Yb	Ka dan Kb
1	200x200	Female	400x400	79009	81000	159979	79876	32488	55326	118237
2	200x200	Female 2	400x400	79009	81000	159979	79876	32488	55326	118237
3	500x500	Female	1000x1000	79009	81000	999983	501098	6985	663509	352912
4	500x500	Female 2	1000x1000	79009	81000	999983	501098	6985	663509	352912
5	200x200	Female	1000x1000	79009	81000	999983	501098	6985	663509	352912
6	200x200	Female 2	1000x1000	79009	81000	999983	501098	6985	663509	352912
7	200x200	Female	400x400	79008	81000	159979	79876	50456	55326	5846
8	200x200	Female	400x400	79009	81001	159979	79876	32488	119659	27887
9	200x200	Female	400x400	79008	81001	159979	79876	50456	119659	124479

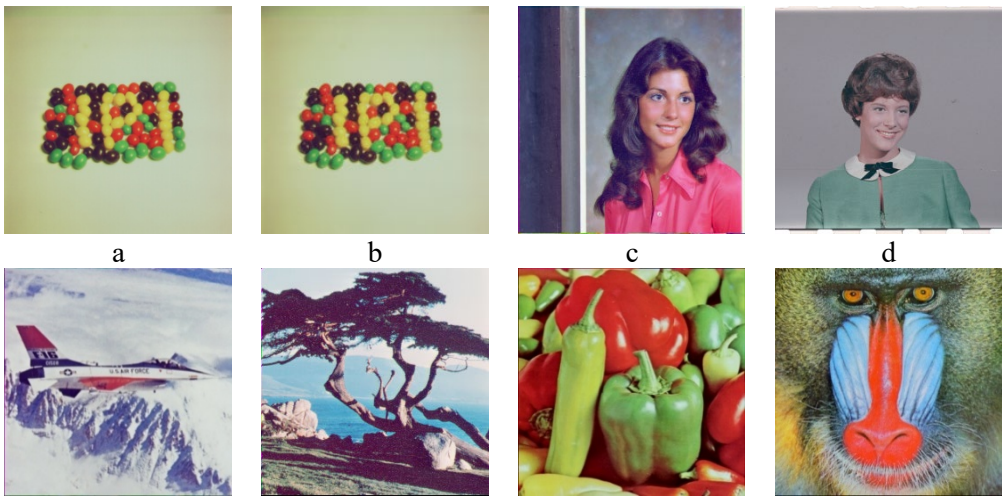
Berdasarkan tabel 1. dalam pembentukan Ka dan Kb atau DHKE dapat dijelaskan sebagai berikut:

1. Dimensi citra sampul dapat mempengaruhi hasil DHKE pada setiap *staging*. Hal ini ditunjukkan oleh hasil uji No.1 dan No.2 terhadap hasil uji No.5 dan No.6.
2. Tidak ada pengaruh dari dimensi citra pesan dan jenis citra sampul terhadap hasil DHKE. Citra sampul yang berbeda tetapi memiliki dimensi yang sama selama tidak terjadi perubahan parameter akan tetap menghasilkan DHKE yang sama. Hal ini ditunjukkan oleh hasil uji No.1 dan No.2 serta No.3 hingga No.6 yang semuanya menghasilkan kunci DHKE identik meskipun dimensi citra pesan dan jenis citra sampul yang digunakan berbeda.
3. Nilai Xa dan Xb yang berbeda dengan dimensi citra sampul yang sama akan menghasilkan nilai DHKE yang berbeda yang dapat dilihat pada No.Uji 7, 8, dan 9.

Pembentukan nilai kunci dalam proses DHKE memiliki pengaruh terhadap dimensi citra sampul dikarenakan penggunaan bilangan prima terbesar dari ukuran citra sampul begitu juga pada proses pencarian median generator modulo yang ada dengan bilangan prima tersebut, oleh karenanya nilai K pada setiap *staging* akan memiliki nilai yang berbeda menyesuaikan dengan dimensi citra sampul yang digunakan.

4.2 Uji MSE Dan PSNR

Pengujian MSE dan PSNR dilakukan untuk mengevaluasi tingkat imperceptibility *stego-image* yang dihasilkan oleh metode *Modified* RESBC dengan generator modulo. Pengujian menggunakan citra pesan dan sampul setiap *staging* (1-3) seperti yang ditunjukkan pada Gambar 8.



Gambar 8. Citra Uji untuk Pengujian MSE dan PSNR (a) Citra pesan Jelly beans 500×500, (b) Citra pesan Jelly beans 200×200, (c) Citra sampul *staging* 1 Female 1200×1200, (d) Citra sampul *staging* 1 Female 2 1200×1200, (e) Citra sampul *staging* 2 Airplane 2800×2800, (f) Citra sampul *staging* 2 Tree 2800×2800, (g) Citra sampul *staging* 3 Peppers 6700×6700, (h) Citra sampul *staging* 3 Mandrill 6700×6700

Parameter kunci DHKE yang digunakan dalam pengujian adalah Xa = 719123 dan Xb = 720456, yang dipilih secara acak dari area nilai tengah luas sampul pertama (1200×1200 = 1440000, sehingga nilai tengah ≈ 720000). Konsistensi parameter ini memastikan bahwa kunci DHKE yang dihasilkan sama untuk setiap *staging* pada semua skenario pengujian.

4.2.1 Hasil Pengujian Staging 1

Hasil pengujian MSE dan PSNR pada *staging* 1 menunjukkan kualitas *stego-image* yang baik untuk kedua ukuran citra pesan. Tabel 2 menampilkan hasil pengujian dengan citra pesan Jelly beans 500×500, sedangkan Tabel 3 menunjukkan hasil dengan citra pesan 200×200.

Tabel 2. Hasil Pengujian MSE dan PSNR *Staging* 1 - Citra Pesan Jelly beans 500×500

SAMPUL 1	LSB	MSE	PSNR
Female.bmp	1	0,324	53,031
	2	0,846	48,858
	3	2,365	44,392
	4	7,344	39,472
Female 2.bmp	1	0,324	53,024
	2	0,849	48,844
	3	2,455	44,230
	4	7,906	39,151

Tabel 3. Hasil Pengujian MSE dan PSNR *Staging* 1 - Citra Pesan Jelly beans 200×200

SAMPUL 1	LSB	MSE	PSNR
Female.bmp	1	0,072	59,530
	2	0,190	55,333
	3	0,544	50,777
	4	1,706	45,812
Female 2.bmp	1	0,073	59,522
	2	0,191	55,314
	3	0,563	50,627
	4	1,801	45,576

Hasil menunjukkan bahwa citra pesan berukuran 200×200 menghasilkan kualitas *stego-image* yang lebih baik dibandingkan citra pesan 500×500. Nilai PSNR tertinggi tercatat sebesar 59,530 dB untuk penyisipan 1 LSB dengan citra pesan 200×200, sedangkan nilai terendah adalah 39,151 dB untuk penyisipan 4 LSB dengan citra pesan 500×500. Semua nilai PSNR yang diperoleh berada di atas ambang batas 30 dB, menunjukkan bahwa metode yang diusulkan mampu mempertahankan kualitas visual yang baik pada *staging* 1.

4.2.2 Hasil Pengujian Staging 2

Pengujian *staging* 2 menunjukkan penurunan kualitas *stego-image* dibandingkan *staging* 1. Tabel 4 menampilkan hasil pengujian dengan citra pesan Jelly beans 500×500, sedangkan Tabel 5 menunjukkan hasil dengan citra pesan 200×200.

Tabel 4. Hasil Pengujian MSE dan PSNR *Staging* 2 - Citra Pesan Jelly beans 500×500

SAMPUL 1	SAMPUL 2	LSB	MSE	PSNR
Female.bmp	Airplane.bmp	1	0,486	51,268
		2	1,327	46,901
		3	3,997	42,114
		4	13,284	36,897
Female 2.bmp	Airplane.bmp	1	0,351	52,682
		2	1,007	48,101
		3	3,165	43,127
		4	11,277	37,609
Female.bmp	Tree.bmp	1	0,486	51,268
		2	1,318	46,931
		3	4,002	42,108
		4	13,490	36,831
Female 2.bmp	Tree.bmp	1	0,351	52,684
		2	1,002	48,123
		3	3,166	43,126
		4	11,445	37,545

Tabel 5. Hasil Pengujian MSE dan PSNR *Staging* 2 - Citra Pesan Jelly beans 200×200

SAMPUL 1	SAMPUL 2	LSB	MSE	PSNR
Female.bmp	Airplane.bmp	1	0,459	51,508
		2	1,215	47,284
		3	3,500	42,690
		4	11,190	37,642
Female 2.bmp	Airplane.bmp	1	0,315	53,144
		2	0,813	49,028
		3	2,309	44,497
		4	7,154	39,585
Female.bmp	Tree.bmp	1	0,459	51,509
		2	1,207	47,312
		3	3,504	42,685
		4	11,374	37,572
Female 2.bmp	Tree.bmp	1	0,315	53,145
		2	0,809	49,051

		3	2,306	44,503
		4	7,241	39,533

Nilai PSNR terbaik sebesar 53,145 dB diperoleh pada penyisipan 1 LSB, sedangkan nilai terendah sebesar 36,831 dB terjadi pada penyisipan 4 LSB. Untuk nilai MSE, diperoleh nilai terendah sebesar 0,315 pada penyisipan 1 LSB dan nilai tertinggi mencapai 13,490 pada penyisipan 4 LSB. Meskipun terjadi penurunan kualitas dibandingkan *staging* 1, semua nilai PSNR masih berada di atas batas minimum 30 dB, menunjukkan bahwa *stego-image* tetap memiliki kualitas visual yang dapat diterima.

Analisis lebih mendalam terhadap hasil *staging* 2 menunjukkan beberapa pola yang konsisten. Pertama, terdapat korelasi yang kuat antara ukuran citra pesan dan kualitas *stego-image* yang dihasilkan, dimana citra pesan berukuran 200×200 *pixel* secara konsisten menghasilkan nilai PSNR yang lebih tinggi dibandingkan dengan citra pesan 500×500 *pixel*. Hal ini disebabkan oleh jumlah data yang lebih sedikit sehingga mengurangi tingkat modifikasi pada citra sampul. Kedua, variasi citra sampul *staging* 2 (Airplane vs Tree) memberikan pengaruh minimal terhadap kualitas akhir, yang terlihat dari selisih PSNR yang kecil pada konfigurasi LSB dan input *staging* 1 yang sama. Hal ini disebabkan oleh *stego-image* hasil *staging* 1 yang menjadi input untuk *staging* 2 memiliki tingkat kompresi yang konsisten, namun disisipkan ke dalam citra sampul yang berbeda dengan karakteristik distribusi warna *pixel* yang bervariasi dan berukuran sama.

4.2.3 Hasil Pengujian Staging 3

Pengujian *staging* 3 menunjukkan tren yang konsisten dengan *staging* sebelumnya, dimana kualitas *stego-image* menurun seiring bertambahnya tingkat *staging*. Pada tahap ini, sistem memproses *stego-image* hasil *staging* 2 sebagai input pesan untuk disispkan ke dalam citra sampul *staging* 3. Tabel 6 menampilkan hasil pengujian dengan citra pesan Jelly beans 500×500, sedangkan Tabel 7 menunjukkan hasil dengan citra pesan 200×200.

Tabel 6. Hasil Pengujian MSE dan PSNR *Staging* 3 - Citra Pesan Jelly beans 500×500

SAMPUL 1	SAMPUL 2	SAMPUL 3	LSB	MSE	PSNR
Female.bmp	Airplane.bmp	Mandrill.bmp	1	0,392	52,194
			2	1,117	47,650
			3	3,379	42,843
			4	11,142	37,661
Female.bmp	Tree.bmp	Mandrill.bmp	1	0,481	51,306
			2	1,396	46,681
			3	4,360	41,736
			4	14,282	36,583
Female 2.bmp	Airplane.bmp	Peppers.bmp	1	0,390	52,224
			2	1,103	47,705
			3	3,306	42,938
			4	10,894	37,759
Female 2.bmp	Tree.bmp	Peppers.bmp	1	0,478	51,338
			2	1,369	46,765

			3	4,288	41,809
			4	13,934	36,690

Tabel 7. Hasil Pengujian MSE dan PSNR *Staging* 3 - Citra Pesan Jelly beans 200×200

SAMPUL 1	SAMPUL 2	SAMPUL 3	LSB	MSE	PSNR
Female.bmp	Airplane.bmp	Mandrill.bmp	1	0,392	52,200
			2	1,105	47,695
			3	3,315	42,926
			4	10,773	37,807
Female.bmp	Tree.bmp	Mandrill.bmp	1	0,481	51,307
			2	1,385	46,717
			3	4,292	41,805
			4	13,868	36,711
Female 2.bmp	Tree.bmp	Peppers.bmp	1	0,476	51,356
			2	1,342	46,853
			3	4,119	41,983
			4	13,016	36,986
Female 2.bmp	Airplane.bmp	Peppers.bmp	1	0,388	52,237
			2	1,074	47,819
			3	3,206	43,071
			4	10,143	38,069

Nilai PSNR pada *staging* 3 berkisar antara 36,583 dB hingga 52,237 dB. Hasil terbaik diperoleh pada penggunaan 1 LSB dengan citra pesan 200×200, sedangkan hasil terendah terjadi pada penggunaan 4 LSB dengan citra pesan 500×500. Meskipun terjadi penurunan kualitas dibandingkan *staging* 1 dan 2, semua nilai PSNR masih memenuhi standar kualitas yang dapat diterima.

4.3 Uji SSIM

Pengujian menggunakan SSIM (*Structural Similarity Index Measure*) terhadap seluruh citra pesan hasil ekstraksi menunjukkan nilai SSIM sebesar 1, yang menandakan kesamaan struktural sempurna antara citra pesan asli dan hasil ekstraksi. Nilai ini mengindikasikan bahwa proses ekstraksi berhasil mengembalikan citra pesan secara utuh tanpa kehilangan informasi maupun degradasi visual.

Nilai SSIM 1 terjadi karena kombinasi algoritma kompresi *lossless* LZW, sistem validasi kunci *Diffie-Hellman* yang akurat, dan penyimpanan informasi *header* yang lengkap (13 *bytes* tetap) yang memungkinkan rekonstruksi citra pesan secara identik *pixel-by-pixel*. Meskipun proses penyisipan menyebabkan sedikit degradasi pada *stego-image* (terlihat dari variasi nilai PSNR 37-59 dB), karakteristik *reversible* dari algoritma RESBC memastikan bahwa setiap bit data pesan dapat diekstraksi dan didekompresi tanpa kehilangan informasi apa pun, sehingga citra pesan hasil ekstraksi memiliki kesamaan struktural 100% dengan citra pesan asli.

4.4 Analisis Perbandingan Metode Steganografi

Metode pembanding yang dipilih merupakan metode yang juga dikaji dalam penelitian ini, yaitu LSB standar [6], LSB2 (2-bit LSB) [7], LSB berbasis PRNG dengan SA-LCG [9], dan RESBC orisinal [8]. Perbandingan langsung secara numerik memiliki keterbatasan akibat perbedaan dataset, ukuran citra

uji, dan kondisi pengujian antar penelitian, sehingga analisis ini bersifat komparatif secara kontekstual. Hasil perbandingan metode steganografi dapat dilihat pada Tabel 8.

Tabel 8. Perbandingan Metode Steganografi

Aspek	LSB Bit Inverse [6]	2LSB [7]	SA-LCG-LSB [9]	RESBC [8]	MRESBC +G.Modulo + DHKE
Pengacakan Posisi Sisip	Tidak ada (Berurutan)	Tidak ada (Berurutan)	SA + LCG	Tidak ada (Berurutan)	Generator Modulo + DHKE
Kompresi Lossless	-	-	-	RLE / HE / SFA / LZW	LZW Konsisten
Multi-Stage Penyisipan	-	-	-	Ya (1-4 *Stage*)	Ya (1-3 *Stage*)
Variasi Bit Sisip	1 bit (tetap)	2 bit (tetap)	1 bit (tetap)	4 bit (tetap)	Fleksibel 1–4 LSB
Metrik Evaluasi	MSE, PSNR	MSE, PSNR	MSE, PSNR	PSNR, HC (*Hiding Capasity*), Pengujin hanya 3 dan 4 *stage*.	MSE, PSNR, SSIM
Pesan-Sampul	RGB 24-bit	Teks - RGB	Binary File - RGB 24-bit	*Grayscale*	RGB 24-bit
PSNR Tertinggi	55,88 dB (*image insertion*)	49,65 dB	84,68 dB (Pesan 41Bytes)	40,95 dB (3 *Stage*, SFA)	59,530 dB (1 LSB, 1 *Stage*)
PSNR Terendah	49,85 dB (*image insertion*)	46,40 dB	67,97 dB (Pesan 1868Bytes)	35,81 dB (4 *Stage*, SFA)	36,583 dB (4 LSB, 3 *Stage*)

Berdasarkan perbandingan pada Tabel 8 di atas, terdapat beberapa perbedaan mendasar antara metode yang diusulkan dengan penelitian-penelitian sebelumnya. Dari sisi keamanan pengacakan, metode [6], [7], dan [8] melakukan penyisipan secara berurutan, sehingga berpotensi dikenali melalui analisis statistik pada area piksel yang berdekatan. Metode [9] telah mengatasi hal ini menggunakan LCG, namun parameter seed LCG bersifat deterministik, yang berarti keamanannya bergantung pada kerahasiaan nilai seed tersebut. Penelitian ini menggunakan Generator Modulo dengan seed yang diturunkan dari DHKE, sehingga nilai awal tidak dapat ditebak tanpa pengetahuan tentang parameter kunci kedua pihak.

Dari sisi evaluasi, keempat penelitian pembanding menggunakan MSE dan PSNR sebagai metrik utama. Nilai PSNR terbaik MRESBC sebesar 59,53 dB mengungguli RESBC orisinal (40,95 dB). Meskipun LSB + PRNG berbasis SA-LCG [9] melaporkan PSNR lebih tinggi terdapat perbedaan mendasar pada pesan yang jauh lebih kecil jika dibandingkan citra pesan pada penelitian ini. Menambahkan SSIM sebagai metrik struktural penelitian ini, yang menghasilkan nilai 1,0 pada seluruh skenario pengujian. Nilai ini mengindikasikan bahwa citra pesan hasil ekstraksi identik secara struktur dengan citra asli, konsisten dengan sifat lossless dari algoritma kompresi LZW yang digunakan. Dari sisi fleksibilitas, metode [6], [7], [8], dan [9] masing-masing menggunakan jumlah bit penyisipan yang

tetap. Penelitian ini memungkinkan variasi 1 hingga 4 bit LSB, yang memberikan pilihan *trade-off* antara kapasitas penyisipan dan kualitas visual sesuai kebutuhan.

5. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan, diperoleh beberapa kesimpulan dari pengamanan citra warna menggunakan *Modified Reversible-Enhanced Stego Block Chaining* dan Generator Modulo sebagai berikut:

1. Peningkatan keamanan berhasil dilakukan melalui penerapan DHKE, generator modulo, dan variasi bit penyisipan, yang menghasilkan posisi sisip tidak berurutan sehingga mempersulit prediksi pola penyisipan. Keamanan kunci diperkuat oleh sifat DHKE yang menghasilkan seed berbeda untuk setiap kombinasi parameter, terbukti dari 9 variasi pengujian parameter yang menghasilkan nilai kunci unik pada setiap konfigurasi.
2. Hasil pengujian dari algoritma RESBC yang dimodifikasi dengan generator modulo dan DHKE menunjukkan bahwa metode yang diusulkan mampu mempertahankan kualitas *stego-image* yang baik dengan nilai PSNR sebesar 45,812 dB untuk penyisipan 4 bit LSB dan nilai PSNR mencapai 59,530 dB untuk penyisipan 1 bit LSB di mana kedua hasil tersebut termasuk nilai PSNR yang baik.

6. SARAN

Berdasarkan penelitian yang telah dilakukan, adapun saran yang dapat digunakan untuk penelitian selanjutnya yang berkaitan, antara lain:

1. Aplikasi dapat dikembangkan sehingga parameter Xa, Xb, dan jumlah bit sisip dapat bervariasi pada tiap *stage* serta variasi *channel* R, G, B untuk penyisipan dapat digunakan.
2. Aplikasi dapat dikembangkan sehingga memiliki fitur enkripsi sebelum gambar disisipkan.

DAFTAR PUSTAKA

[1] K. Bansal, A. Agrawal, and N. Bansal, "A Survey on Steganography using Least Significant bit (LSB) Embedding Approach," *Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020)*, pp. 64–69, Jun. 2020.

[2] D. R. I. M. Setiadi, "Payload enhancement on least significant bit image steganography using edge area dilation," *International Journal of Electronics and Telecommunications*, vol. 65, no. 2, pp. 287–292, 2019, doi: 10.24425/ijet.2019.126312.

[3] E. H. Rachmawanto, D. R. I. M. Setiadi, C. A. Sari, P. N. Andono, O. Farooq, and N. Pradita, "Spread Embedding Technique in LSB Image Steganography based on Chaos Theory," *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)*, pp. 39–44, 2019.

[4] D. R. I. M. Setiadi, D. N. Aini, S. N. Putro, E. H. Rachmawanto, and C. A. Sari, "Survey of Methods in the Spatial Domain Image Steganography based Imperceptibility and Payload Capacity," *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2019.

[5] J. C. Kurniawan, A. Nugraha, A. I. Prayogo, and T. F. Novanto, "Improving Data Embedding Capacity in LSB Steganography Utilizing LSB2 and Zlib Compression," *Sinkron: Jurnal dan Penelitian Teknik Informatika*, vol. 9, no. 1, pp. 174–181, Jan. 2024, doi: 10.33395/sinkron.v9i1.13185.

[6] F. I. Lubis, S. Suwilo, and P. Sihombing, "Analysis of LSB Algorithm Modification with Bit Inverse and Insertion based on Length of Message," *International Conference on Culture Heritage, Education, Sustainable Tourism, and Innovation Technologies (CESIT 2020)*, pp. 522–529, Mar. 2021, doi: 10.5220/0010333505220529.

[7] F. N. Hakim and M. Sholikhan, "Enhancing Data Security through Digital Image Steganography: An Implementation of the Two Least Significant Bits (2LSB) Method," *International Journal of Graphic Design (IJGD)*, vol. 2, no. 2, pp. 222–235, Nov. 2024, doi: 10.51903/ijgd.v2i2.2124.

[8] S. Khan, M. A. Irfan, A. Arif, A. Ali, Z. A. Memon, and A. Khaliq, "Reversible-Enhanced Stego Block Chaining Image Steganography: A Highly Efficient Data Hiding Technique," *Canadian Journal of Electrical and Computer Engineering*, vol. 43, no. 2, pp. 66–72, Mar. 2020, doi: 10.1109/CJECE.2019.2938844.

[9] M. J. Bawaneh, F. Al-Shalabi, and O. M. Al-Hazaimeh, "A Novel RGB Image Steganography Using Simulated Annealing and LCG via LSB," *IJCSNS International Journal of Computer Science and Network Security*, vol. 21, no. 1, Jan. 2021, doi: 10.22937/IJCSNS.2021.21.1.19.

[10] S. Rani, A. Kurniawardhani, and Y. A. W. Rendani, "Steganography on Digital Color Image Using Modulo Function and Pseudo-Random Number Generator," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 11, no. 6, pp. 2470–2475, 2021, doi: 10.18517/ijaseit.11.6.12687.

[11] P. K. Baidoo, "Comparative Analysis of the Compression of Text Data Using Huffman, Arithmetic, Run-Length, and Lempel Ziv Welch Coding Algorithms," *Journal of Advances in Mathematics and Computer Science*, vol. 38, no. 9, pp. 144–156, Aug. 2023, doi: 10.9734/jamcs/2023/v38i91812.

[12] C. G. Aprillia and A. Prapanca, "Perbandingan Citra Digital Sebelum dan Sesudah Melakukan Kombinasi Proses Enkripsi Menggunakan Algoritma RC4 dengan Metode Steganografi Least Significant Bit (LSB)," *Journal of Informatics and Computer Science*, vol. 04, no. 1, 2022, [Online]. Available: www.petitcolas.net.

[13] A. Oluwaseun. Modupe, A. E. Adedoyin, and A. O. Titilayo, "A Comparative Analysis of LSB, MSB and PVD Based Image Steganography," *International Journal of Research and Review*, vol. 8, no. 9, pp. 373–377, Sep. 2021, doi: 10.52403/ijrr.20210948.

[14] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method," *IEEE Access*, vol. 10, pp. 124053–124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

[15] K. Yulion *et al.*, "STEGANOGRAFI METODE INVERTED LSB MENGGUNAKAN POLA ADAPTIF DAN DCT," *Jurnal Informatika & Rekayasa Elektronika(JIRE)*, vol. 7, no. 2, Nov. 2024, [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

[16] A. D. Molato and F. B. Calanda, "A Secured LSB-Based Image Steganography using Modified Collatz Conjecture," *2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023*, pp. 1997–2002, 2023, doi: 10.1109/ICACCS57279.2023.10113029.

[17] G. Alomari and A. Aljarah, "Efficiency of Using the Diffie-Hellman Key in Cryptography for Internet Security," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 6, pp. 2039–2044, 2021.

[18] A. Kumar, P. Sufian Hameed, D. Hellman, and K. Exchange, "Diffie Hellman Stand the Test of Time (Protocol's Limitations, Applications and Functional Divergence) General Terms," *Int. J. Comput. Appl.*, vol. 176, no. 31, pp. 975–8887, Jun. 2020.

[19] R. Rimani, N. H. Said, A. Ali-Pacha, and O. Ozer, "Key exchange based on Diffie-Hellman protocol and image registration," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, pp. 1751–1758, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1751-1758.

[20] C. K. Deo, D. K. Singh, A. Singh, and N. K. Soni, "Developing a Highly Secure and High Capacity LSB Steganography Technique using PRNG," *2020 International Conference on Computational Performance (ComPE)*, vol. 2, no. 4, pp. 136–140, Jul. 2020.

[21] I. Haverkamp and D. K. Sarmah, "Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis," *Int. J. Inf. Secur.*, vol. 23, no. 4, pp. 2607–2635, Aug. 2024, doi: 10.1007/s10207-024-00853-9.