

## Implementation of Rabin cryptography and parity-based pixel-difference steganography for hiding text messages in PNG images

Reynaza Azhura<sup>1</sup>, Muhammad Haris<sup>2</sup>

<sup>1,2</sup>Program Studi Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Indonesia  
Email: [ashurareynaza@gmail.com](mailto:ashurareynaza@gmail.com); [muhammadharis@umsu.ac.id](mailto:muhammadharis@umsu.ac.id)

### ABSTRAK

Penelitian ini bertujuan mengimplementasikan kriptografi Rabin dan steganografi berbasis paritas selisih piksel untuk menyisipkan serta memulihkan pesan teks pada citra PNG. Penelitian dilakukan secara eksperimental melalui pengembangan aplikasi web lokal berbasis PHP dan pengujian fungsional black-box. Pesan dikodekan menggunakan ASCII dan dienkripsi dengan operasi kuadrat modular Rabin. Ciphertext kemudian disisipkan dengan menyesuaikan paritas selisih kanal biru pasangan piksel. Proses ekstraksi dan dekripsi digunakan untuk memulihkan pesan asli. Pengujian dengan pesan PIN:121314 serta bilangan prima 383 dan 503 menghasilkan modulus publik 192649 dan sepuluh nilai ciphertext. Verifikasi modular memperlihatkan kesesuaian hasil enkripsi dan pemilihan kandidat dekripsi. Pada 30 pasangan piksel contoh, 13 pasangan mengalami perubahan kanal biru dan 17 pasangan mempertahankan nilainya. Pesan asli berhasil diperoleh kembali, dan seluruh delapan skenario pengujian fungsional menghasilkan keluaran sesuai harapan. Hasil tersebut menunjukkan keberhasilan integrasi enkripsi, penyisipan, ekstraksi, dan dekripsi dalam satu aplikasi pengolahan pesan berbasis citra.

**Kata Kunci:** kriptografi Rabin; steganografi; paritas selisih piksel; citra PNG; pengujian black-box

### ABSTRACT

*This study implemented Rabin cryptography and pixel-difference parity-based steganography to embed and recover text messages in PNG images. An experimental approach was adopted by developing a PHP-based local web application and evaluating its functions through black-box testing. The messages were encoded using ASCII and encrypted through Rabin modular squaring. The resulting ciphertext was embedded by adjusting the parity of blue-channel differences between adjacent pixel pairs. Extraction and decryption were performed to reconstruct the original plaintext. Testing with PIN:121314 and prime numbers 383 and 503 generated a public modulus of 192649 and ten ciphertext values. Modular verification confirmed the encryption results and the selection of decryption candidates. Among 30 documented pixel pairs, 13 required blue-channel adjustment while 17 retained their original values. The original message was successfully recovered, and all eight functional test scenarios produced the expected outputs. The findings demonstrate the integration of encryption, embedding, extraction, and decryption within a single image-based message processing application.*

**Keywords:** Rabin cryptography; steganography; pixel-difference parity; PNG images; black-box testing

### Corresponding Author:

Reynaza Azhura,  
Universitas Muhammadiyah Sumatera Utara,  
Jl. Kapten Mukhtar Basri No. 3, Glugur Darat II, Kecamatan Medan Timur,  
Kota Medan, Sumatera Utara 20238, Indonesia  
Email: [ashurareynaza@gmail.com](mailto:ashurareynaza@gmail.com)



## 1. INTRODUCTION

Perkembangan teknologi informasi telah meningkatkan kemudahan dalam pertukaran data melalui berbagai media digital, termasuk penyampaian pesan teks dan distribusi citra. Di sisi lain, kemudahan tersebut menimbulkan kebutuhan terhadap mekanisme perlindungan informasi, khususnya ketika pesan mengandung

data yang hanya boleh diketahui oleh pihak tertentu. Pengamanan pesan tidak hanya berkaitan dengan upaya mencegah isi informasi dibaca oleh pihak yang tidak berwenang, tetapi juga dapat dilakukan dengan menyembunyikan keberadaan pesan di dalam media digital. Dua pendekatan yang dapat digunakan untuk memenuhi kebutuhan tersebut adalah kriptografi dan steganografi. Kriptografi mengubah pesan asli menjadi bentuk tersandi melalui suatu algoritma dan kunci, sedangkan steganografi menyisipkan informasi ke dalam media penampung agar keberadaan pesan tidak terlihat secara langsung. Penggabungan kedua pendekatan tersebut memungkinkan pesan memperoleh perlindungan melalui proses penyandian sebelum disembunyikan pada media digital (Kumbhakar et al., 2023; Alanzy et al., 2023).

Citra digital dapat dimanfaatkan sebagai media steganografi melalui penyesuaian nilai piksel untuk menyimpan informasi tambahan. Metode *Least Significant Bit* (LSB) menempatkan bit pesan pada posisi terendah suatu nilai piksel. Jebur et al. (2023) mengkaji penyembunyian informasi dengan LSB, sedangkan Rahman et al. (2025) mengembangkan variasi substitusi LSB. Kajian Alenizi et al. (2024) dan Murthy dan Hegde (2024) menempatkan teknik penyisipan serta pengamanan pesan sebagai komponen penting steganografi citra. Naveen dan Jayaraghavi (2024) serta Panigrahi dan Padhy (2025) menunjukkan keragaman pendekatan penyisipan pada gambar digital. Perbedaan karakteristik metode tersebut menjadi pertimbangan dalam memilih mekanisme penyisipan yang sesuai dengan tujuan sistem.

Penggabungan kriptografi dan steganografi telah diterapkan dalam berbagai penelitian. Saragih et al. (2023) memadukan ElGamal dan LSB, sedangkan Kumbhakar et al. (2023) menerapkan pendekatan cryptostegano untuk pengamanan informasi. Alanzy et al. (2023) mengembangkan penyisipan citra dengan enkripsi hibrida, sementara Pardosi et al. (2024) mengkaji Playfair, ElGamal, dan LSB. Wildan dan Ashari (2024) memadukan pembangkitan nilai menggunakan *Linear Congruential Generator*, AES-CBC, dan steganografi. Kadhem dan Baawi (2023) juga menggabungkan penyisipan citra dengan komponen pengodean serta enkripsi. Temuan-temuan tersebut memperlihatkan bahwa penyandian pesan dan penyimpanan informasi pada citra dapat dirancang sebagai dua tahap yang saling melengkapi.

Selain LSB, penyisipan dapat memanfaatkan hubungan intensitas dua piksel bertetangga. Wu dan Tsai (2003) memperkenalkan *Pixel Value Differencing* (PVD), yang menggunakan rentang selisih piksel sebagai dasar jumlah bit yang ditempatkan. Pengembangan teknik penyisipan adaptif, termasuk yang dibahas Aljughaiman dan Alrawashdeh (2026), memperlihatkan pentingnya karakteristik piksel dalam perancangan steganografi. Penelitian ini menggunakan paritas selisih kanal biru dari pasangan piksel untuk merepresentasikan satu bit ciphertext pada setiap pasangan. Dengan demikian, mekanisme yang diterapkan adalah penyisipan berbasis paritas selisih, yang perlu dibedakan dari PVD adaptif berdasarkan interval selisih.

Algoritma Rabin merupakan metode kriptografi kunci publik yang memanfaatkan operasi kuadrat modular dengan modulus hasil perkalian dua bilangan prima (Rabin, 1979). Dekripsinya menghasilkan kandidat akar modular yang direkonstruksi menggunakan Chinese Remainder Theorem dan diseleksi berdasarkan aturan pengodean pesan. Azzahra et al. (2024) membahas implementasi Rabin pada layanan pesan berbasis bot, sedangkan Manalu et al. (2024) membandingkan performa Rabin dengan beberapa skema enkripsi lain. Karakteristik operasi modular dan kebutuhan pemilihan kandidat menjadikan algoritma ini relevan sebagai komponen penyandian pesan dalam aplikasi steganografi.

Penelitian ini mengintegrasikan enkripsi Rabin dan penyisipan berbasis paritas selisih kanal biru pada citra PNG dalam aplikasi web lokal. Kontribusinya terletak pada perancangan alur utuh dari pembentukan kunci, enkripsi, penyisipan ciphertext, ekstraksi, hingga dekripsi yang disertai pemeriksaan matematis dan pengujian fungsional. Pendekatan ini memperluas pilihan implementasi kriptografi-steganografi dengan menggabungkan pemulihan plaintext dan pengolahan citra dalam satu sistem.

Penelitian ini mengimplementasikan sistem berbasis web lokal menggunakan bahasa pemrograman PHP dengan citra berformat *Portable Network Graphics* (PNG) sebagai media penampung pesan. Penggunaan PNG dipilih untuk mendukung penyimpanan perubahan nilai piksel tanpa kehilangan data akibat kompresi lossy. Proses sistem diawali dengan pembentukan kunci dan enkripsi pesan menggunakan algoritma Rabin, dilanjutkan dengan penyisipan ciphertext ke dalam citra melalui penyesuaian paritas selisih nilai pasangan piksel. Pada proses pemulihan, data yang disisipkan diekstraksi dari citra stego untuk memperoleh ciphertext, kemudian dilakukan dekripsi menggunakan parameter kunci yang sesuai. Sistem dirancang agar seluruh tahapan tersebut dapat dioperasikan melalui antarmuka aplikasi.

Tujuan penelitian ini adalah mengimplementasikan algoritma Rabin bersama teknik paritas selisih piksel untuk penyembunyian pesan teks pada citra PNG serta menguji keberhasilan proses enkripsi, penyisipan, ekstraksi, dan dekripsi. Evaluasi dilakukan melalui penelusuran hasil perhitungan modular, perubahan paritas pasangan piksel, pemulihan pesan, dan pengujian fungsi aplikasi terhadap masukan yang sesuai maupun tidak sesuai.

## 2. RESEARCH METHOD

### A. Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental melalui implementasi perangkat lunak untuk mengintegrasikan algoritma kriptografi Rabin dan teknik steganografi berbasis paritas selisih piksel. Pendekatan tersebut digunakan untuk mengamati proses perubahan pesan teks menjadi ciphertext, penyisipan ciphertext pada citra digital, ekstraksi data tersembunyi, serta pemulihan pesan ke bentuk semula. Penelitian difokuskan pada pengujian mekanisme penyandian dan penyembunyian pesan melalui aplikasi yang dikembangkan berbasis web lokal.

Pelaksanaan penelitian terdiri atas empat tahapan utama, yaitu analisis kebutuhan sistem, perancangan alur pengolahan pesan, implementasi algoritma, dan pengujian fungsional aplikasi. Analisis kebutuhan dilakukan untuk menentukan masukan, proses, dan keluaran sistem. Perancangan sistem menggunakan diagram alur dan pemodelan *Unified Modeling Language* (UML) sebagai dasar hubungan antara pengguna dengan fungsi aplikasi. Selanjutnya, algoritma Rabin diintegrasikan dengan mekanisme penyisipan berdasarkan paritas selisih pasangan piksel. Tahap akhir dilakukan melalui pengujian fungsional untuk mengetahui kesesuaian keluaran aplikasi dengan fungsi yang telah ditentukan.

Secara operasional, penelitian dibagi menjadi dua proses yang saling berhubungan. Proses pertama meliputi pembentukan kunci, enkripsi pesan, dan penyisipan ciphertext ke dalam citra PNG. Proses kedua meliputi ekstraksi ciphertext dari citra stego, dekripsi menggunakan parameter kunci yang sesuai, serta pemulihan pesan teks asli.

### B. Data Penelitian dan Lingkungan Implementasi

Data penelitian berupa pesan teks yang diproses menggunakan algoritma Rabin dan gambar digital berformat *Portable Network Graphics* (PNG) sebagai media penyisipan. Pesan teks menjadi masukan proses enkripsi, sedangkan citra asli (*cover image*) digunakan untuk menampung representasi biner ciphertext. Setelah proses penyisipan selesai, sistem menghasilkan citra stego (*stego image*) yang dapat disimpan dan digunakan dalam proses ekstraksi.

Pengujian utama menggunakan pesan PIN:121314 dengan pasangan bilangan prima  $p = 383$  dan  $q = 503$  serta gambar PNG bernama mobil.png sebagai media penampung. Konfigurasi tersebut menjadi dasar analisis enkripsi, penempatan bit, ekstraksi ciphertext, dan pemulihan plaintext pada hasil penelitian.

Tabel 1. Parameter dan lingkungan implementasi penelitian

| Komponen                    | Spesifikasi                     |
|-----------------------------|---------------------------------|
| Jenis data                  | Pesan teks dan citra digital    |
| Format gambar               | PNG                             |
| Contoh pesan                | PIN:121314                      |
| Bilangan prima p            | 383                             |
| Bilangan prima q            | 503                             |
| Modulus publik n            | 192649                          |
| Metode enkripsi             | Rabin                           |
| Teknik penyisipan           | Paritas selisih pasangan piksel |
| Kanal penyisipan            | Biru (Blue Channel)             |
| Bahasa pemrograman          | PHP                             |
| Server lokal                | Apache melalui XAMPP            |
| Sistem operasi pengembangan | Windows 11                      |
| Pengembangan antarmuka      | Bootstrap 5                     |
| Peramban pengujian          | Google Chrome                   |

Pengembangan sistem dilakukan menggunakan Visual Studio Code sebagai penyunting kode program. Aplikasi dijalankan melalui Apache Web Server pada lingkungan XAMPP dan diakses menggunakan peramban web. Penggunaan lingkungan lokal bertujuan mendukung proses pengembangan dan pengujian tanpa mengharuskan aplikasi dipublikasikan melalui server internet.

### C. Perancangan Alur Pengolahan Pesan

Perancangan aplikasi dilakukan dengan menghubungkan algoritma enkripsi dan mekanisme penyisipan citra dalam satu rangkaian proses. Pada tahap pengiriman, pengguna memasukkan pesan teks, gambar PNG, serta dua bilangan prima sebagai parameter kunci. Sistem membentuk modulus publik berdasarkan kedua bilangan prima tersebut, kemudian mengenkripsi pesan menggunakan algoritma Rabin.

Hasil enkripsi berupa ciphertext dikonversi menjadi representasi biner untuk disisipkan ke dalam citra. Penyisipan dilakukan dengan memanfaatkan paritas selisih nilai kanal biru pada dua piksel yang berdekatan. Proses tersebut menghasilkan citra stego yang memuat informasi hasil enkripsi.

Pada tahap penerimaan, pengguna memasukkan citra stego serta pasangan bilangan prima yang digunakan sebelumnya. Sistem melakukan ekstraksi bit dari citra, merekonstruksi ciphertext, kemudian menjalankan proses dekripsi Rabin. Hasil dekripsi selanjutnya dikonversi menjadi karakter teks untuk memperoleh kembali pesan asli.

Dengan demikian, alur utama sistem terdiri atas proses berikut:

- 1) Enkripsi dan penyisipan:  
Plaintext → Pembentukan Kunci → Enkripsi Rabin → Ciphertext → Representasi Biner → Penyisipan pada Citra PNG → Citra Stego.
- 2) Ekstraksi dan dekripsi:  
Citra Stego → Pembacaan Pasangan Piksel → Ekstraksi Bit → Ciphertext → Dekripsi Rabin → Pemulihan Karakter → Plaintext.

#### **D. Pembentukan Kunci dan Proses Enkripsi Rabin**

Algoritma Rabin merupakan metode kriptografi kunci publik yang menggunakan operasi kuadrat modular untuk mengenkripsi informasi. Proses dekripsi dilakukan dengan memanfaatkan faktor prima modulus dan pencarian akar kuadrat modular (Rabin, 1979).

Pembentukan kunci dimulai dengan menentukan dua bilangan prima berbeda, yaitu  $p$  dan  $q$ . Kedua bilangan tersebut digunakan untuk menghitung modulus publik  $n$  melalui persamaan:

$$n = p \times q \quad (1)$$

Dalam penelitian ini, contoh parameter yang digunakan adalah  $p = 383$  dan  $q = 503$  sehingga diperoleh  $n = 192649$ . Pasangan bilangan tersebut memenuhi kondisi  $p \equiv 3 \pmod{4}$  dan  $q \equiv 3 \pmod{4}$ , yang memungkinkan penggunaan rumus akar kuadrat modular pada proses dekripsi Rabin.

Pesan direpresentasikan sebagai nilai ASCII, kemudian setiap karakter  $a_i$  dikodekan dengan redundansi numerik  $M_i = (a_i \times 256) + a_i = 257a_i$ . Nilai  $M_i$  selanjutnya digunakan sebagai masukan enkripsi Rabin. Pola ini juga digunakan untuk memilih kandidat akar pada tahap dekripsi.

$$M_i = (a_i \times 256) + a_i = 257a_i \quad (2)$$

dengan  $M_i$  merupakan bilangan hasil pengodean karakter ke- $i$  dan  $a_i$  merupakan nilai ASCII karakter tersebut. Pembentukan nilai  $M_i$  bertujuan memberikan pola pengodean yang dapat digunakan dalam menentukan kandidat plaintext setelah proses dekripsi.

Nilai  $M_i$  kemudian dienkripsi menggunakan kunci publik  $n$  dengan persamaan:

$$C_i = M_i^2 \pmod{n} \quad (3)$$

dengan  $C_i$  merupakan ciphertext untuk karakter ke- $i$ . Operasi tersebut dilakukan terhadap karakter pesan sehingga diperoleh rangkaian nilai ciphertext yang menjadi masukan proses penyisipan. Nilai ciphertext kemudian direpresentasikan dalam bentuk biner untuk diolah pada tahap steganografi.

Pola pengodean  $M_i = 257a_i$  memberikan penanda numerik untuk menentukan kandidat plaintext setelah operasi akar modular. Pengodean tersebut dipertahankan secara konsisten antara proses enkripsi dan dekripsi.

#### **E. Penyisipan Ciphertext Berdasarkan Paritas Selisih Piksel**

Penyisipan dilakukan melalui penyesuaian paritas selisih nilai kanal biru pada pasangan piksel. Gagasan pemanfaatan selisih piksel berkaitan dengan pendekatan PVD oleh Wu dan Tsai (2003). Pada aplikasi ini, setiap pasangan merepresentasikan satu bit dengan aturan paritas, sedangkan PVD adaptif klasik menentukan banyaknya bit berdasarkan rentang selisih.

Pada tahap awal, ciphertext yang dihasilkan oleh algoritma Rabin direpresentasikan sebagai deretan bit. Citra penampung kemudian dibaca untuk memperoleh nilai kanal biru dari pasangan piksel yang berdekatan. Apabila nilai kedua piksel dinyatakan sebagai  $B_1$  dan  $B_2$ , selisih absolut keduanya dihitung menggunakan:

$$d = |B_2 - B_1| \quad (4)$$

Selanjutnya, nilai paritas selisih diperoleh melalui:

$$h = d \pmod{2} \quad (5)$$

dengan  $h$  menyatakan paritas selisih piksel. Nilai  $h$  dibandingkan dengan bit ciphertext  $b$  yang akan disisipkan.

Apabila  $h = b$ , pasangan piksel tidak memerlukan perubahan karena paritas selisih telah merepresentasikan bit pesan yang diinginkan. Sebaliknya, apabila  $h \neq b$ , nilai salah satu kanal biru disesuaikan sehingga selisih akhir memenuhi kondisi:

$$|B_2' - B_1| \pmod{2} = b \quad (6)$$

dengan  $B_2'$  merupakan nilai kanal biru piksel kedua setelah penyesuaian.

Sebagai contoh, pasangan kanal biru  $B_1 = 0$  dan  $B_2 = 0$  memiliki selisih awal 0. Untuk bit pesan bernilai 1, nilai kanal kedua diubah menjadi 1 sehingga paritas selisih menjadi 1. Jika bit pesan bernilai 0, nilai kedua piksel tetap dipertahankan.

Proses pemeriksaan dan penyesuaian paritas dilakukan terhadap pasangan piksel yang digunakan untuk menampung bit-bit ciphertext. Setelah penyisipan selesai, citra hasil pengolahan disimpan dalam format PNG dan digunakan sebagai masukan pada proses ekstraksi.

### F. Ekstraksi Ciphertext dari Citra Stego

Ekstraksi merupakan proses pengambilan kembali informasi yang sebelumnya disisipkan ke dalam citra stego. Pada tahap ini, sistem menerima gambar PNG hasil penyisipan dan membaca nilai kanal biru dari pasangan piksel sesuai urutan pengolahan data yang diterapkan aplikasi.

Setiap pasangan piksel digunakan untuk memperoleh kembali satu bit melalui penghitungan paritas selisih, yaitu:

$$b_i = |B_{2i} - B_{1i}| \bmod 2 \quad (7)$$

dengan  $b_i$  merupakan bit hasil ekstraksi dari pasangan piksel ke- $i$ .

Bit-bit yang berhasil diperoleh kemudian direkonstruksi menjadi representasi ciphertext. Rangkaian ciphertext tersebut menjadi masukan proses dekripsi Rabin. Keberhasilan tahap ekstraksi dinilai berdasarkan kemampuan sistem memperoleh informasi ciphertext dan meneruskannya ke tahap dekripsi.

Bit-bit hasil ekstraksi digabungkan kembali menjadi rangkaian data ciphertext dalam urutan pembacaan pasangan piksel. Nilai ciphertext yang direkonstruksi kemudian digunakan pada proses dekripsi Rabin untuk memperoleh kembali pesan teks.

### G. Dekripsi Rabin dan Pemulihan Pesan

Proses dekripsi bertujuan mengembalikan ciphertext menjadi representasi pesan awal menggunakan pasangan bilangan prima  $p$  dan  $q$ . Dalam algoritma Rabin, satu ciphertext pada umumnya menghasilkan empat kandidat akar kuadrat modular. Oleh karena itu, proses pemulihan memerlukan penghitungan kandidat dan pemilihan representasi pesan yang sesuai dengan pola pengodean awal.

Untuk parameter  $p$  dan  $q$  yang masing-masing memenuhi kondisi kongruensi 3 modulo 4, akar kuadrat ciphertext  $C$  terhadap kedua bilangan prima dapat dihitung melalui:

$$M_p = C^{\frac{p+1}{4}} \bmod p \quad (8)$$

$$M_q = C^{\frac{q+1}{4}} \bmod q \quad (9)$$

Selanjutnya, invers modular ditentukan menggunakan:

$$y_p = q^{-1} \bmod p \quad (10)$$

$$y_q = p^{-1} \bmod q \quad (11)$$

Keempat kandidat plaintext direkonstruksi menggunakan Chinese Remainder Theorem (CRT), yaitu:

$$r_1 = (y_p q M_p + y_q p M_q) \bmod n \quad (12)$$

$$r_2 = (-r_1) \bmod n \quad (13)$$

$$r_3 = (y_p q M_p - y_q p M_q) \bmod n \quad (14)$$

$$r_4 = (-r_3) \bmod n \quad (15)$$

Nilai  $r_1$  sampai  $r_4$  merepresentasikan kandidat hasil dekripsi dari ciphertext yang sama. Pemilihan kandidat dilakukan dengan memperhatikan pola representasi bilangan yang digunakan sebelum enkripsi. Dalam contoh penelitian, nilai karakter dikodekan menggunakan  $M_i = 257a_i$ , sehingga kandidat yang sesuai dengan pola tersebut dapat dikonversi kembali menjadi nilai ASCII.

Pemilihan kandidat didasarkan pada pola pengodean  $M_i = 257a_i$  dengan  $a_i$  sebagai kode karakter. Kandidat yang sesuai dikonversi ke karakter ASCII dan disusun menurut urutan ciphertext sehingga membentuk kembali pesan asli.

### H. Pengujian Fungsional Sistem

Pengujian aplikasi dilakukan menggunakan metode *black-box testing* untuk memeriksa kesesuaian fungsi sistem berdasarkan masukan dan keluaran yang dihasilkan. Pengujian difokuskan pada dua kelompok proses, yaitu enkripsi dan penyisipan pesan serta ekstraksi dan dekripsi pesan.

Respons aplikasi dievaluasi melalui hubungan antara masukan, proses, dan keluaran yang diharapkan. Skenario mencakup masukan valid, pesan kosong, gambar yang tidak dipilih, format tidak sesuai, keberadaan data pesan, dan pasangan kunci yang tepat maupun tidak tepat.

Tabel 2. Skenario pengujian fungsional aplikasi

| No. | Skenario pengujian                 | Keluaran yang diharapkan                         |
|-----|------------------------------------|--------------------------------------------------|
| 1   | Pesan dan citra PNG valid          | Enkripsi dan penyisipan dapat diproses           |
| 2   | Pesan kosong                       | Sistem menampilkan pesan kesalahan               |
| 3   | Citra penampung tidak dipilih      | Sistem menampilkan pesan kesalahan               |
| 4   | Format gambar selain PNG           | Sistem menolak berkas                            |
| 5   | Citra stego valid                  | Data tersembunyi dapat diekstraksi               |
| 6   | Gambar biasa tanpa data pesan      | Sistem memberikan informasi data tidak ditemukan |
| 7   | Parameter $p$ dan $q$ sesuai       | Pesan asli dapat ditampilkan kembali             |
| 8   | Parameter $p$ dan $q$ tidak sesuai | Pesan tidak dapat didekripsi secara benar        |

Setiap skenario diperiksa berdasarkan kesesuaian respons aktual sistem dengan keluaran yang diharapkan. Hasil pengujian kemudian digunakan untuk menilai keberhasilan fungsi aplikasi pada kondisi yang dicantumkan dalam Tabel 2.

Delapan skenario tersebut digunakan untuk menilai fungsi utama aplikasi, termasuk penanganan masukan tidak valid dan keberhasilan pemulihan pesan pada kondisi pengujian.

### **I. Teknik Analisis Hasil Pengujian**

Analisis hasil penelitian dilakukan secara deskriptif dengan menelaah keluaran proses enkripsi, penyisipan, ekstraksi, dekripsi, dan pengujian fungsional aplikasi. Analisis proses kriptografi dilakukan melalui pemeriksaan hubungan antara karakter plaintext, hasil pengodean numerik, ciphertext, serta kandidat hasil dekripsi menggunakan persamaan Rabin.

Pada proses steganografi, analisis diarahkan pada perubahan nilai kanal biru pasangan piksel sebagaimana dicatat dalam tabel penyisipan dan ekstraksi. Pemeriksaan dilakukan untuk mengetahui apakah paritas selisih akhir sesuai dengan bit pesan yang diproses dan apakah sistem dapat memperoleh kembali ciphertext dari media stego.

Kesesuaian proses pemulihan pesan diamati melalui perbandingan antara pesan teks awal dan keluaran dekripsi. Sementara itu, hasil pengujian fungsional dianalisis berdasarkan keberhasilan atau kegagalan respons aplikasi terhadap delapan skenario pengujian yang telah ditentukan.

Hasil analisis dikelompokkan menurut keterkaitan antar-tahap pengolahan data. Ketepatan enkripsi dan dekripsi ditinjau dari kesesuaian perhitungan modular; penyisipan dan ekstraksi ditinjau dari kecocokan nilai bit; sedangkan respons antarmuka dinilai menggunakan hasil delapan skenario pengujian fungsional. Ketiga aspek tersebut digunakan untuk menjelaskan kinerja operasional sistem secara terintegrasi.

## **3. RESULTS AND DISCUSSION**

### **A. Hasil Implementasi Aplikasi**

Penelitian ini menghasilkan aplikasi berbasis web lokal yang mengintegrasikan proses enkripsi pesan menggunakan algoritma Rabin dengan penyisipan data pada citra digital melalui penyesuaian paritas selisih piksel. Implementasi aplikasi dikembangkan menggunakan bahasa pemrograman PHP dengan dukungan Apache Web Server melalui XAMPP. Sistem menyediakan dua fungsi utama, yaitu enkripsi dan penyisipan pesan serta ekstraksi dan dekripsi pesan. Kedua fungsi tersebut diakses melalui antarmuka yang memungkinkan pengguna memasukkan parameter kunci, pesan teks, dan gambar berformat PNG.

Pada halaman enkripsi dan penyisipan, pengguna memasukkan dua bilangan prima, yaitu  $p$  dan  $q$ , yang digunakan untuk membentuk modulus publik algoritma Rabin. Pengguna kemudian memasukkan pesan rahasia dan memilih citra penampung. Berdasarkan dokumentasi implementasi, aplikasi memproses masukan tersebut untuk menghasilkan ciphertext dan citra stego yang dapat diunduh. Hasil enkripsi ditampilkan dalam bentuk deretan bilangan, sedangkan citra stego ditampilkan sebagai keluaran proses penyisipan.

Halaman ekstraksi dan dekripsi digunakan untuk mengambil kembali pesan yang telah disisipkan. Pengguna memasukkan citra stego berformat PNG beserta pasangan parameter kunci yang sesuai. Aplikasi kemudian melakukan ekstraksi data tersembunyi, mengembalikan representasi ciphertext, dan menjalankan dekripsi Rabin. Hasil proses ditampilkan dalam dua bentuk, yaitu ciphertext hasil ekstraksi dan plaintext hasil pemulihan.

Antarmuka enkripsi–penyisipan dan ekstraksi–dekripsi bekerja dalam alur aplikasi yang saling terhubung. Pengguna memperoleh keluaran berupa citra stego setelah penyisipan serta ciphertext dan plaintext setelah ekstraksi dan dekripsi. Hasil ini memperlihatkan terselenggaranya proses pengolahan pesan dari masukan hingga pemulihan dalam satu sistem. Hasil kedua proses diperlihatkan pada Gambar 1 dan Gambar 2.



Gambar 1. Hasil enkripsi ciphertext dan citra stego pada aplikasi.

Gambar 2. Hasil ekstraksi ciphertext dan pemulihan plaintext.

### B. Hasil Pembentukan Kunci dan Enkripsi Rabin

Pengujian proses enkripsi dilakukan menggunakan pesan teks PIN:121314 dengan parameter bilangan prima  $p = 383$  dan  $q = 503$ . Berdasarkan Persamaan (1), kedua bilangan tersebut menghasilkan modulus publik  $n = 192649$ . Modulus ini digunakan pada proses enkripsi masing-masing karakter setelah karakter dikonversi menjadi representasi numerik.

Konversi pesan dilakukan menggunakan kode ASCII. Setiap karakter kemudian diberi pola redundansi berdasarkan Persamaan (2), yaitu  $M = 257a$ , dengan  $a$  merupakan nilai ASCII karakter. Nilai  $M$  selanjutnya dienkripsi menggunakan operasi  $C = M^2 \bmod n$ . Penghitungan ini menghasilkan satu nilai ciphertext untuk setiap karakter pesan.

Sebagai contoh, karakter P memiliki kode ASCII 80 sehingga diperoleh  $M = (80 \times 256) + 80 = 20560$ . Enkripsi menggunakan persamaan  $C = M^2 \bmod n$  menghasilkan  $C = 20560^2 \bmod 192649 = 41694$ . Hasil perhitungan untuk kesepuluh karakter disajikan pada Tabel 3.

Tabel 3. Hasil enkripsi karakter pesan menggunakan algoritma Rabin

| No. | Karakter | ASCII | Nilai M | Ciphertext |
|-----|----------|-------|---------|------------|
| 1   | P        | 80    | 20560   | 41694      |
| 2   | I        | 73    | 18761   | 5398       |
| 3   | N        | 78    | 20046   | 168951     |
| 4   | :        | 58    | 14906   | 64539      |
| 5   | 1        | 49    | 12593   | 33522      |
| 6   | 2        | 50    | 12850   | 22307      |
| 7   | 1        | 49    | 12593   | 33522      |
| 8   | 3        | 51    | 13107   | 143190     |
| 9   | 1        | 49    | 12593   | 33522      |
| 10  | 4        | 52    | 13364   | 10873      |

Berdasarkan Tabel 3, seluruh karakter berhasil direpresentasikan sebagai bilangan ciphertext menggunakan operasi kuadrat modular. Pesan yang semula berbentuk PIN:121314 diubah menjadi rangkaian ciphertext berikut:

41694,5398,168951,64539,33522,22307,33522,143190,33522,10873

Hasil tersebut memperlihatkan bahwa setiap karakter diproses secara individual. Karakter yang sama menghasilkan nilai ciphertext identik ketika dienkripsi dengan parameter dan pola pengodean yang sama. Hal ini terlihat pada karakter 1 yang muncul sebanyak tiga kali dan seluruhnya menghasilkan ciphertext 33522.

Kesamaan ciphertext untuk karakter 1 yang berulang merupakan konsekuensi langsung dari sifat deterministik operasi kuadrat modular dan pengodean karakter yang digunakan. Hasil tersebut juga menunjukkan konsistensi proses enkripsi pada nilai ASCII yang sama. Dalam konteks penerapan lebih luas, penentuan skema pengodean dan pengelolaan kunci merupakan unsur penting dalam perancangan sistem kriptografi.

Modulus  $n = 192649$  digunakan untuk menampilkan tahapan perhitungan Rabin secara rinci. Secara matematis, keluaran enkripsi memenuhi persamaan kuadrat modular dan dapat ditelusuri kembali melalui pencarian akar dengan kunci privat. Dasar operasi tersebut sejalan dengan konstruksi kriptografi yang dikemukakan Rabin (1979).

### C. Hasil Penyisipan Ciphertext pada Citra PNG

Ciphertext hasil enkripsi direpresentasikan dalam bentuk bit dan ditempatkan pada kanal biru pasangan piksel citra PNG. Selisih absolut pasangan piksel dihitung, kemudian paritasnya dibandingkan dengan bit pesan yang akan disisipkan.

Pada setiap pasangan, nilai kanal biru dipertahankan apabila paritas selisih telah sama dengan bit ciphertext. Jika paritas berbeda, kanal piksel kedua disesuaikan hingga selisih akhir memenuhi bit yang ditetapkan pada Persamaan (4)–(6).



### E. Hasil Dekripsi Rabin dan Pemulihan Pesan

Hasil ekstraksi selanjutnya diproses menggunakan algoritma Rabin untuk memperoleh kembali pesan asli. Proses dekripsi dilakukan melalui penghitungan akar kuadrat modular terhadap dua faktor prima modulus, penentuan invers modular, dan penggabungan hasil menggunakan *Chinese Remainder Theorem* (CRT).

Pengujian dekripsi menggunakan parameter yang sama dengan proses enkripsi, yaitu  $p = 383$ ,  $q = 503$ , dan  $n = 192649$ . Sebagai contoh, ciphertext pertama bernilai 41694 yang berasal dari karakter P. Berdasarkan Persamaan (8) dan Persamaan (9), penghitungan akar modular yang benar menghasilkan:

$$M_p = 41694^{96} \bmod 383 = 261$$

$$M_q = 41694^{126} \bmod 503 = 63$$

Selanjutnya, nilai invers modular diperoleh sebagai berikut:

$$y_p = 503^{-1} \bmod 383 = 233$$

$$y_q = 383^{-1} \bmod 503 = 197$$

Nilai tersebut digunakan dalam Persamaan (12) sampai Persamaan (15) untuk memperoleh empat kandidat akar Rabin, yaitu 87585, 105064, 20560, dan 172089.

Keempat kandidat tersebut memiliki hubungan matematis dengan ciphertext yang sama. Namun, hanya nilai 20560 yang memenuhi pola pengodean karakter P dalam contoh penelitian, yaitu  $M = 257 \times 80$ . Dengan demikian, nilai ASCII yang diperoleh adalah 80 dan karakter yang dipulihkan adalah P.

Penghitungan akar modular untuk ciphertext lainnya menghasilkan kandidat yang tercantum pada Tabel 5. Kandidat yang memenuhi pola  $M = 257a$  kemudian digunakan untuk memperoleh nilai ASCII dan karakter yang sesuai.

Tabel 5 menyajikan kandidat akar modular untuk delapan karakter berbeda yang terdapat dalam pesan uji. Karakter 1 yang muncul berulang menghasilkan kandidat akar yang sama karena memiliki ciphertext identik.

Tabel 5. Hasil verifikasi kandidat akar Rabin dan pemulihan karakter

| Karakter | Ciphertext | Empat kandidat akar Rabin    | Kandidat terpilih |
|----------|------------|------------------------------|-------------------|
| P        | 41694      | 87585, 105064, 20560, 172089 | 20560             |
| I        | 5398       | 76606, 116043, 173888, 18761 | 18761             |
| N        | 168951     | 20046, 172603, 13152, 179497 | 20046             |
| :        | 64539      | 177743, 14906, 153231, 39418 | 14906             |
| 1        | 33522      | 6557, 186092, 180056, 12593  | 12593             |
| 2        | 22307      | 65665, 126984, 179799, 12850 | 12850             |
| 3        | 143190     | 179542, 13107, 124773, 67876 | 13107             |
| 4        | 10873      | 13364, 179285, 8768, 183881  | 13364             |

Berdasarkan Tabel 5, setiap ciphertext pada contoh pengujian menghasilkan empat kandidat akar. Kandidat yang sesuai dengan pola pengodean selanjutnya dikonversi kembali menjadi nilai ASCII. Setelah seluruh karakter dipulihkan sesuai urutan, diperoleh pesan:

PIN:121314

Hasil tersebut sama dengan plaintext yang digunakan pada proses enkripsi. Dokumentasi aplikasi juga memperlihatkan ciphertext hasil ekstraksi dan pesan asli yang berhasil ditampilkan kembali. Dengan demikian, rangkaian proses enkripsi, penyisipan, ekstraksi, dan dekripsi berhasil mengembalikan pesan contoh sesuai dengan masukan awal.

Pemilihan kandidat merupakan tahapan penting pada algoritma Rabin karena satu ciphertext dapat menghasilkan empat akar modular. Pola numerik 257a memungkinkan kandidat untuk pesan uji diidentifikasi sehingga karakter dapat dikembalikan dalam urutan yang sama dengan plaintext masukan.

### F. Hasil Pengujian Fungsional Menggunakan Black-Box Testing

Pengujian fungsional dilakukan untuk menilai apakah fungsi aplikasi menghasilkan keluaran sesuai dengan kebutuhan yang telah ditentukan. Metode yang digunakan adalah black-box testing dengan fokus pada respons sistem terhadap kondisi masukan yang berbeda. Pengujian dibagi menjadi dua kelompok, yaitu proses enkripsi dan penyisipan serta proses ekstraksi dan dekripsi.

Kelompok pertama mencakup pengujian masukan pesan dan gambar PNG yang valid, penanganan pesan kosong, penanganan gambar yang tidak dipilih, serta penolakan format gambar selain PNG. Kelompok kedua mencakup pengujian citra stego yang valid, penggunaan gambar tanpa data tersembunyi, penggunaan parameter kunci yang sesuai, serta penggunaan parameter kunci yang tidak sesuai.

Rangkuman hasil pengujian fungsional disajikan pada Tabel 6.

Tabel 6. Hasil pengujian fungsional aplikasi

| No. | Skenario pengujian   | Keluaran yang diharapkan         | Hasil    |
|-----|----------------------|----------------------------------|----------|
| 1   | Pesan dan PNG valid  | Enkripsi dan penyisipan berhasil | Berhasil |
| 2   | Pesan kosong         | Pesan kesalahan ditampilkan      | Berhasil |
| 3   | Gambar tidak dipilih | Pesan kesalahan ditampilkan      | Berhasil |
| 4   | Gambar bukan PNG     | Berkas ditolak                   | Berhasil |

(Reynaza Azhura)

| No. | Skenario pengujian             | Keluaran yang diharapkan                   | Hasil    |
|-----|--------------------------------|--------------------------------------------|----------|
| 5   | Citra stego valid              | Pesan tersembunyi diekstraksi              | Berhasil |
| 6   | Gambar biasa                   | Informasi data tidak ditemukan ditampilkan | Berhasil |
| 7   | Parameter p dan q sesuai       | Pesan asli berhasil ditampilkan            | Berhasil |
| 8   | Parameter p dan q tidak sesuai | Pesan tidak dapat didekripsi secara benar  | Berhasil |

Tabel 6 menunjukkan bahwa delapan skenario pengujian memberikan keluaran sesuai harapan. Empat skenario pertama mengevaluasi fungsi enkripsi–penyisipan dan validasi masukan, sedangkan empat skenario berikutnya mengevaluasi fungsi ekstraksi–dekripsi serta pemilihan parameter kunci.

Pengujian dengan parameter kunci yang tidak sesuai menghasilkan kondisi pemulihan pesan yang tidak benar, sedangkan parameter yang sesuai menghasilkan plaintext yang diharapkan. Hasil tersebut memperlihatkan peran pasangan kunci dalam konsistensi alur dekripsi.

Delapan skenario memberikan gambaran fungsional sistem pada operasi normal maupun penanganan masukan yang tidak memenuhi persyaratan. Keberhasilan setiap skenario dinilai berdasarkan respons aplikasi terhadap keluaran yang telah ditetapkan.

Secara keseluruhan, hasil black-box testing mengonfirmasi bahwa fungsi utama aplikasi berjalan sesuai dengan skenario operasional yang dirancang.

#### **G. Pembahasan Integrasi Metode dan Implikasi Implementasi**

Hasil implementasi dan pengujian menunjukkan bahwa kombinasi kriptografi Rabin dengan penyisipan berbasis paritas selisih piksel dapat digunakan untuk membangun aplikasi penyembunyian pesan pada citra digital. Proses Rabin berfungsi mengubah representasi pesan sebelum disisipkan, sedangkan proses steganografi digunakan untuk menempatkan ciphertext pada media citra. Kedua mekanisme tersebut bekerja pada tahap yang berbeda dan saling terhubung dalam alur pengolahan pesan.

Hasil penelitian ini sejalan dengan arah pendekatan Saragih et al. (2023) dan Alanzy et al. (2023), yang memadukan tahap enkripsi serta penyisipan informasi pada citra. Perbedaanannya terletak pada penggunaan algoritma Rabin untuk penyandian karakter dan penyesuaian paritas selisih pasangan piksel sebagai media bit ciphertext. Kombinasi tersebut menyediakan alur terintegrasi dari plaintext hingga citra stego dan kembali menjadi plaintext.

Proses enkripsi memberikan representasi numerik ciphertext, sedangkan mekanisme penyisipan menempatkan representasi tersebut pada kanal citra. Kedua tahap menghasilkan fungsi perlindungan yang berbeda tetapi saling melengkapi dalam rancangan aplikasi.

Pada tahap Rabin, persamaan kuadrat modular menghasilkan ciphertext yang konsisten terhadap nilai masukan dan kunci yang sama. Tahap dekripsi menggunakan empat akar modular dan aturan pengodean karakter untuk memilih representasi plaintext. Karakteristik tersebut memperlihatkan keterkaitan antara desain representasi pesan dan keberhasilan pemulihan karakter.

Pada tahap penyisipan, perbandingan paritas selisih memungkinkan satu bit ciphertext ditempatkan pada setiap pasangan kanal biru. Contoh perubahan dari 0 menjadi 1 menunjukkan mekanisme penyesuaian kanal ketika paritas awal tidak sesuai. Penggunaan perubahan lokal yang terukur memudahkan penelusuran hubungan antara nilai piksel dan bit pesan.

Format PNG digunakan untuk mempertahankan nilai kanal piksel dalam berkas hasil penyisipan. Kesenambungan data bit pada proses ekstraksi memungkinkan ciphertext direkonstruksi sebelum didekripsi dengan pasangan kunci yang sesuai.

Analisis representasi data memperlihatkan bahwa deretan bilangan ciphertext dapat diproses sebagai karakter numerik dan tanda pemisah, kemudian diubah menjadi bit penyisipan. Keterkaitan antara panjang data, urutan bit, serta hasil ekstraksi menjadi bagian penting dalam pengolahan pesan pada citra.

Integrasi kedua tahap menghasilkan aplikasi yang dapat mengolah pesan melalui pembentukan kunci, enkripsi, penyisipan, ekstraksi, dan dekripsi. Hasil perhitungan Rabin, kesesuaian paritas piksel, serta delapan skenario fungsional yang berhasil menunjukkan keterlaksanaan rancangan pada data uji yang digunakan. Penelitian ini memberikan contoh implementasi kriptografi–steganografi yang dapat dikembangkan melalui variasi parameter kunci, media citra, dan pengujian kinerja secara lebih luas.

## **4. CONCLUSION**

Penelitian ini menghasilkan aplikasi web lokal berbasis PHP yang mengintegrasikan algoritma Rabin dengan penyisipan ciphertext melalui paritas selisih kanal biru pasangan piksel pada citra PNG. Pengujian menggunakan pesan PIN:121314 dengan  $p = 383$  dan  $q = 503$  menghasilkan modulus  $n = 192649$  dan sepuluh ciphertext yang sesuai dengan operasi kuadrat modular. Proses ekstraksi dan dekripsi berhasil memulihkan pesan menjadi plaintext semula. Analisis terhadap 30 pasangan piksel contoh memperlihatkan 13 pasangan memerlukan penyesuaian kanal biru, sedangkan 17 pasangan telah memenuhi paritas bit yang disisipkan.

Seluruh delapan skenario black-box testing menghasilkan respons aplikasi sesuai dengan keluaran yang ditetapkan.

Temuan tersebut menunjukkan bahwa operasi penyandian, penyisipan, pemulihan data, dan validasi masukan dapat dijalankan secara terintegrasi. Pengembangan berikutnya dapat difokuskan pada pengelolaan kunci, pengodean pesan, serta evaluasi kualitas dan ketahanan citra untuk memperluas penerapan sistem.

## REFERENSI

- Alanzzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. M. (2023). Image steganography using LSB and hybrid encryption algorithms. *Applied Sciences*, 13(21), Article 11771. <https://doi.org/10.3390/app132111771>
- Alenizi, A., Mohammadi, M. S., Al-Hajji, A. A., & Ansari, A. S. (2024). A review of image steganography based on multiple hashing algorithm. *Computers, Materials & Continua*, 80(2), 2463–2494. <https://doi.org/10.32604/cmc.2024.051826>
- Aljughaiman, A., & Alrawashdeh, R. (2026). Content-adaptive LSB steganography with saliency fusion, ACO dispersion, and hybrid encryption with ablation study. *Scientific Reports*, 16, Article 3829. <https://doi.org/10.1038/s41598-025-33920-9>
- Azzahra, F., Girinoto, & Setyawan, F. G. (2024). Implementasi Rabin public key cryptosystem dalam skema enkripsi dekripsi pesan dengan Telegram Bot. *Info Kripto*, 18(3), 111–117. <https://doi.org/10.56706/ik.v18i3.113>
- Jebur, S. A., Nawar, A. K., Kadhim, L. E., & Jahefer, M. M. (2023). Hiding information in digital images using LSB steganography technique. *International Journal of Interactive Mobile Technologies*, 17(7), 167–178. <https://doi.org/10.3991/ijim.v17i07.38737>
- Kadhem, E. L., & Baawi, S. S. (2023). A secure and high capacity image steganography approach using Huffman coding and RSA encryption. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, 15(2), 35–50. <https://doi.org/10.29304/jqcm.2023.15.2.1231>
- Kumbhakar, D., Sanyal, K., & Karforma, S. (2023). An optimal and efficient data security technique through crypto-stegano for E-commerce. *Multimedia Tools and Applications*, 82(14), 21005–21018. <https://doi.org/10.1007/s11042-023-14526-7>
- Manalu, D. C. R., Enjelina, M., & Sipayung, J. B. J. (2024). Perbandingan performance kriptografi RSA, RSA-CRT, Rabin dalam proses pengamanan pesan berbasis teks. *Jurnal Quancom: Quantum Computer Jurnal*, 2(2), 23–30. <https://doi.org/10.62375/jqc.v2i2.417>
- Murthy, N. N., & Hegde, V. (2024). Secure data hiding: A comprehensive LSB-based steganography framework with cryptographic enhancements. In *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*. IEEE. <https://doi.org/10.1109/CSITSS64042.2024.10817051>
- Naveen, P., & Jayaragavi, R. (2024). Image steganography method for securing multiple images using LSB–GA. *Wireless Personal Communications*, 135(1), 1–19. <https://doi.org/10.1007/s11277-024-10945-3>
- Panigrahi, R., & Padhy, N. (2025). An effective steganographic technique for hiding the image data using the LSB technique. *Cyber Security and Applications*, 3, Article 100069. <https://doi.org/10.1016/j.csa.2024.100069>
- Pardosi, S. S. P., Manik, M., & Situmorang, I. M. (2024). Pengujian dan analisis teknik steganografi menggunakan metode Playfair, ElGamal, dan LSB untuk menyembunyikan data pada gambar digital dalam aplikasi modern. *Jurnal Quancom: Quantum Computer Jurnal*, 2(2), 17–22. <https://doi.org/10.62375/jqc.v2i2.422>
- Rabin, M. O. (1979). *Digitalized signatures and public-key functions as intractable as factorization* (MIT/LCS/TR-212). Massachusetts Institute of Technology, Laboratory for Computer Science. <https://hdl.handle.net/1721.1/149499>
- Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., de la Torre Díez, I., Ramírez Vargas, D. L., & Martínez Espinosa, J. C. (2025). A novel and efficient digital image steganography technique using least significant bit substitution. *Scientific Reports*, 15, Article 107. <https://doi.org/10.1038/s41598-024-83147-3>
- Saragih, E., Siregar, D., & Dafitri, H. (2023). Implementasi penyisipan pesan teks terenkripsi menggunakan kriptografi ElGamal pada citra digital menggunakan steganografi LSB. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, 22(2), 464–473. <https://doi.org/10.53513/jis.v22i2.8755>
- Wildan, M., & Ashari, W. M. (2024). Text data security using LCG and CBC with steganography technique on digital image. *Journal of Applied Informatics and Computing*, 8(2), 400–407. <https://doi.org/10.30871/jaic.v8i2.8457>
- Wu, D.-C., & Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24(9–10), 1613–1626. [https://doi.org/10.1016/S0167-8655\(02\)00402-6](https://doi.org/10.1016/S0167-8655(02)00402-6)