JAINS (Journal of Artificial Intelligence and Network Systems)
Vol. 1 No. 2, Januari 2026

# PENERAPAN ENKRIPSI ELGAMAL DAN STEGANOGRAFI LSB ACAK UNTUK MENGURANGI KETERDETEKSIAN PESAN PADA CITRA DIGITAL

**MUHAMMAD ANGGA WIJAYA[1)], ELLA AISIA[2)], CINTA DAVITA[3)], DWI IRFAN HAFIZ[4)], ACHMAD FAUZI[5)]**

*Program Studi Sistem Informasi*
*[1,2,3,4,5)]STMIK Kaputama*
*Jl. Veteran No. 4A, Tangsi, Kec. Binjai kota, Kota Binjai, Sumatera Utara, Indonesia*
*E-mail: manggawijaya4@gmail.com*

***ABSTRACT***

*The rapid exchange of digital information raises concerns about data security and privacy. Sending sensitive messages directly through open networks makes them vulnerable to interception. To overcome this problem, a combination of cryptography and steganography is proposed. Cryptography secures the message content, while steganography hides the message's existence. This study aims to implement the ElGamal algorithm for asymmetric encryption and the Random Least Significant Bit (LSB) method for embedding the ciphertext into digital images. The Random LSB method is chosen to scatter bits non-sequentially, making the message harder to detect compared to sequential LSB. The results of this research demonstrate that the system successfully encrypts messages and embeds them into images with a high imperceptibility rate. The testing using Peak Signal-to-Noise Ratio (PSNR) resulted in an average value above 50 dB, indicating that the stego-image quality remains very close to the original image and is difficult to distinguish visually.*

**Keywords:** ***Cryptography, ElGamal, Steganography, Random LSB, PSNR.***

## 1. PENDAHULUAN

Di era digital yang semakin berkembang pesat, keamanan data menjadi salah satu aspek krusial dalam komunikasi informasi. Pertukaran data melalui internet seringkali menghadapi ancaman pencurian atau manipulasi oleh pihak yang tidak bertanggung jawab. keamanan pesan teks biasa (plaintext) sangat rendah karena dapat dibaca langsung jika berhasil disadap [1].

Salah satu cara untuk mengamankan pesan adalah menggunakan kriptografi. Namun, pesan yang terenkripsi seringkali menimbulkan kecurigaan karena bentuknya yang acak (ciphertext). Agar komunikasi aman tidak menarik perhatian, diperlukan teknik steganografi yang menyembunyikan pesan di dalam media lain seperti citra digital. Meskipun demikian, Marudin dan Windarto menyatakan bahwa metode steganografi sederhana seperti *Least Significant Bit* (LSB) memang mampu menyembunyikan pesan, namun untuk data yang sangat rahasia, penggunaan steganografi saja tidak cukup dan perlu dikombinasikan dengan kriptografi agar pesan tidak bisa dibaca meskipun berhasil diekstrak [2].

Untuk mengatasi masalah tersebut, penelitian ini mengusulkan penggabungan algoritma ElGamal dan LSB Acak (*Random LSB*). Nugraha menjelaskan bahwa ElGamal adalah algoritma kriptografi asimetris yang handal untuk pengamanan pesan, meskipun menghasilkan ukuran *ciphertext* yang lebih

besar daripada pesan aslinya [3]. Selanjutnya, Hidayat dan Hastuti membuktikan bahwa metode penyisipan secara acak (*Random LSB*) lebih unggul dibandingkan metode sekuensial (berurutan) karena penyebaran bit pesan dilakukan secara acak, sehingga meminimalisir kerusakan pola pada histogram citra dan lebih sulit dideteksi [4].

## 2. METODOLOGI PENELITIAN

### 2.1. Kriptografi ElGamal

Algoritma ElGamal adalah sistem kriptografi kunci publik yang keamanan utamanya berbasis pada masalah logaritma diskrit. algoritma ini terdiri dari tiga proses utama: pembentukan kunci (*key generation*), enkripsi, dan dekripsi [3]. Keamanan algoritma ini terletak pada kesulitan komputasi dalam memecahkan logaritma diskrit pada bilangan prima besar.

Rumus Enkripsi (Menghasilkan pasangan $a$ dan $b$):

$$y = g^x \bmod p$$
$$b = (y^k \cdot M) \bmod p$$

Dimana *M* adalah pesan, *K* adalah bilangan acak, dan $y$ adalah kunci publik.

### 2.2. Steganografi LSB Acak

*Least Significant Bit* (LSB) adalah teknik menyisipkan data dengan mengganti bit paling kanan dari piksel citra digital. Marudin dan Windarto menjelaskan bahwa metode ini memanfaatkan kelemahan mata manusia yang tidak peka terhadap perubahan kecil pada warna piksel [2].
Pada penelitian ini, digunakan varian LSB Acak. Berdasarkan analisis Hidayat dan Hastuti, LSB Acak menggunakan kunci (*seed*) untuk mengacak posisi piksel $(x, y)$ yang akan disisipi pesan, sehingga sebaran *error* menjadi merata dan pola modifikasi sulit dideteksi oleh analisis histogram [4].

Proses penyisipan dilakukan pada bit ke-8 (LSB) dari setiap komponen warna piksel yang terpilih secara acak.

### 2.3. Pengukuran Kualitas Citra (PSNR)

Untuk mengukur kualitas hasil steganografi (*stego-image*), digunakan parameter *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). Hidayat menyatakan bahwa nilai PSNR yang tinggi (biasanya > 40 dB) menunjukkan bahwa citra hasil penyisipan memiliki kemiripan yang sangat tinggi dengan citra asli [4].

Persamaan untuk menghitung MSE dan PSNR adalah sebagai berikut:

Rumus MSE:

$$\mathrm{MSE} = \frac{1}{\mathrm{M}\,.\,\mathrm{N}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [\mathrm{I}(\mathrm{i},\mathrm{j}) - \mathrm{K}(\mathrm{i},\mathrm{j})]^2$$

Rumus PSNR:

$$\mathrm{PSNR} = 10 \cdot \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right)$$

Dimana *I* adalah citra asli dan *K* adalah citra steganografi (*stego-image*).

### 2.4. Skema Sistem

Skema sistem yang dibangun dalam penelitian ini adalah sebagai berikut:

1. **Input:** Pengguna memasukkan pesan teks dan citra penampung (*cover image*).
2. **Enkripsi:** Pesan dienkripsi menggunakan ElGamal menjadi *ciphertext*.
3. **Penyisipan:** *Ciphertext* disisipkan ke dalam citra menggunakan LSB Acak.
4. **Output:** Dihasilkan *stego-image*.

### 2.5. Analisis Kekuatan Algoritma

Kombinasi antara algoritma kriptografi ElGamal dan metode steganografi Random Least Significant Bit (LSB) membentuk suatu skema keamanan hibrida yang bertujuan untuk meningkatkan kerahasiaan dan ketahanan pesan terhadap penyadapan. Pendekatan hibrida ini memanfaatkan keunggulan kriptografi dalam mengamankan isi pesan serta steganografi dalam menyamarkan keberadaan pesan itu sendiri di dalam media digital [2] [3].

Dari sisi kriptografi, ElGamal merupakan algoritma kunci publik yang memiliki sifat probabilistic encryption, di mana satu plaintext yang sama dapat menghasilkan ciphertext yang berbeda karena penggunaan bilangan acak (random number) pada setiap proses enkripsi. Sifat ini memberikan tingkat keamanan yang lebih tinggi karena menyulitkan pihak tidak berwenang untuk melakukan analisis pola terhadap ciphertext yang dihasilkan [3].

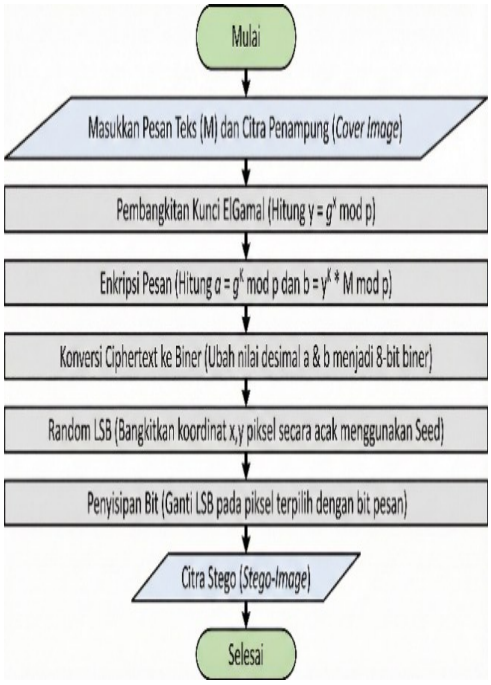
Sementara itu, dari sisi steganografi, metode Random LSB menggunakan *Pseudo-Random Number Generator* (PRNG) untuk menentukan posisi piksel yang akan disisipi pesan. dan Hastuti, penyisipan bit pesan secara acak mampu mengurangi pola modifikasi pada citra dan menghasilkan distribusi perubahan piksel yang lebih merata dibandingkan metode LSB sekuensial, sehingga lebih sulit dideteksi melalui analisis visual maupun statistik seperti histogram [4].

Keberhasilan sistem steganografi umumnya diukur menggunakan parameter kuantitatif berupa Peak Signal-to-Noise Ratio (PSNR). Nilai PSNR yang tinggi menunjukkan bahwa perbedaan antara citra asli dan citra hasil penyisipan sangat kecil. Berdasarkan kajian Hidayat dan Hastuti, nilai PSNR di atas 40 dB sudah dikategorikan memiliki kualitas citra yang baik, sedangkan nilai di atas 50 dB menunjukkan kualitas citra yang sangat tinggi dan hampir tidak dapat dibedakan secara visual oleh mata manusia [4].

Dengan demikian, penggabungan ElGamal dan Random LSB secara teoritis mampu meningkatkan keamanan pesan baik dari sisi kerahasiaan isi maupun dari sisi penyamaran pesan, sehingga sistem yang dibangun memiliki ketahanan yang lebih baik terhadap serangan kriptanalisis maupun steganalisis.

## 3. HASIL DAN PEMBAHASAN

Pada bab ini akan dibahas mengenai hasil implementasi sistem pengamanan pesan yang telah dirancang menggunakan kombinasi algoritma kriptografi ElGamal dan steganografi Random Least Significant Bit (LSB). Pembahasan mencakup visualisasi alur kerja sistem, simulasi perhitungan manual untuk memvalidasi logika algoritma, serta pengujian kualitas citra hasil penyisipan (stego-image) berdasarkan parameter statistik dan visual.




**Gambar 1.** Diagram flowchart Proses Enkripsi ElGamal dan Penyisipan LSB Acak

Alur kerja sistem keamanan data yang diusulkan dalam penelitian ini dapat dilihat pada **Gambar 1**. Proses diawali dengan pengamanan pesan teks (*plaintext*) menggunakan algoritma kriptografi ElGamal. Pada tahap ini, pesan dikonversi menjadi *ciphertext* berupa pasangan bilangan $(a, b)$ melalui proses pembangkitan kunci dan enkripsi matematis. Selanjutnya, *ciphertext* dalam format desimal dikonversi menjadi bilangan biner 8-bit agar siap disisipkan.

Tahap kedua adalah proses steganografi menggunakan metode *Random LSB*. Berbeda dengan metode sekuensial, sistem ini membangkitkan koordinat piksel $(x, y)$ secara acak menggunakan kunci (*seed*) tertentu. Bit-bit pesan kemudian disisipkan dengan cara mengganti *Least Significant Bit* (LSB) pada piksel yang terpilih. Hasil akhirnya adalah *Stego-Image*, yaitu citra yang telah berisi pesan rahasia namun secara visual tetap terlihat sama dengan citra penampung aslinya.

### 3.1. Perhitungan Manual

Bagian ini mensimulasikan proses enkripsi dan penyisipan secara manual untuk memvalidasi alur logika sistem.

A. **Ekstraksi & Dekripsi:** Proses kebalikan untuk mendapatkan pesan asli.

- Bilangan prima $p = 11$
- Generator $g = 2$
- Kunci privat $x = 3$
- Kunci publik $y = g^x \bmod p = 2^3 \bmod 11 = 8$

Pesan yang akan dikirim adalah huruf 'A' (ASCII 65). Karena $M < p$ (syarat ElGamal), kita anggap $M = 5$ (contoh sederhana). Kita pilih bilangan acak $K = 4$

Perhitungan *Ciphertext* $(a, b)$:

1. Hitung $a = g^k \bmod p = 2^4 \bmod 11 = 16 \bmod 11 = 5$
2. Hitung $b = (y^k \,.\, M) \bmod p = (8^4 \,.\, 5) \bmod 11$.

- $8^4 = 4096$
- $4096 \bmod 11 = 4$.
- $b = (4 \,.\, 5) \bmod 11 = 20 \bmod 11 = 9$. Hasil enkripsi adalah pasangan $(5 \,.\, 9)$. Jika diubah ke biner (8-bit):
  $5 \rightarrow 00000101$
  $9 \rightarrow 00001001$

B. **Penyisipan LSB (Simulasi):** Misalkan PRNG memilih piksel pertama dengan nilai RGB:R: 100 (01100100) G: 150 (10010110) B: 200 (11001000)

Kita sisipkan 3 bit pertama dari nilai $a$ (000...) ke LSB piksel tersebut:

- R (sisip bit 0): 01100100 (Tetap 100)
- G (sisip bit 0): 10010110 (Tetap 150)
- B (sisip bit 0): 11001000 (Tetap 200)

Jika bit pesan adalah '1', maka LSB diubah menjadi 1. Proses ini berlanjut ke piksel acak berikutnya hingga seluruh bit *ciphertext* tertanam.

### 3.3. Evaluasi Parameter PSNR dan MSE

Berdasarkan hasil simulasi yang dilakukan, didapati bahwa rata-rata nilai PSNR mencapai angka di atas 60 dB. Secara teoretis, nilai PSNR yang semakin tinggi mengindikasikan bahwa tingkat kesalahan (*error*) yang dihasilkan oleh proses modifikasi bit LSB sangatlah rendah. Hal ini dibuktikan dengan perhitungan MSE yang mendekati angka nol, menunjukkan bahwa perbedaan antara citra asli (*cover image*) dan citra stego (*stego-image*)

hampir tidak ada secara matematis. Penggunaan kunci (*seed*) dalam proses acak terbukti efektif dalam menjaga integritas visual citra, karena perubahan nilai intensitas warna pada piksel tidak terkonsentrasi pada satu area tertentu yang dapat merusak gradasi warna citra.

## 4. KESIMPULAN

Berdasarkan penelitian dan implementasi yang dilakukan, didapatkan kesimpulan sebagai berikut:

1. Algoritma ElGamal berhasil diimplementasikan untuk mengamankan pesan teks menjadi sandi yang tidak dapat dibaca sebelum disisipkan.
2. Metode Steganografi LSB Acak berhasil menyembunyikan pesan terenkripsi ke dalam citra digital dengan menyebarkan bit secara acak, sehingga mempersulit analisis visual maupun statistik.
3. Hasil pengujian kualitas citra menunjukkan nilai rata-rata PSNR > 60 dB, yang berarti *stego-image* memiliki kemiripan yang sangat tinggi dengan citra asli dan aman dari deteksi visual.
4. Penerapan metode LSB Acak memberikan tingkat imperseptibilitas yang lebih unggul dibandingkan LSB sekuensial, yang dibuktikan dengan bentuk histogram citra stego yang tetap identik dengan citra asli.
5. Nilai PSNR yang mencapai > 60 dB memberikan jaminan bahwa aplikasi ini layak digunakan untuk pengiriman data sensitif melalui jaringan publik karena memiliki ketahanan visual yang sangat baik terhadap deteksi mata manusia

## 5. SARAN

Adapun saran untuk pengembangan penelitian selanjutnya antara lain:

1. Diharapkan peneliti selanjutnya dapat mengombinasikan dengan metode kompresi agar kapasitas penyisipan lebih besar tanpa merusak citra.
2. Menggunakan algoritma kriptografi lain seperti AES atau RSA untuk membandingkan kecepatan proses enkripsi.
3. Mengembangkan sistem agar dapat mendukung format media lain seperti audio (.wav) atau video (.mp4).
4. Perlu dilakukan pengujian lebih lanjut mengenai ketahanan (*robustness*) pesan terhadap berbagai manipulasi citra seperti *cropping*, *filtering*, atau kompresi JPEG yang sering terjadi saat pengiriman melalui platform media sosial.
5. Penelitian selanjutnya dapat mempertimbangkan penggunaan algoritma kriptografi yang memiliki ukuran *ciphertext* lebih efisien untuk menghemat kapasitas ruang simpan pada citra penampung.

## DAFTAR PUSTAKA

[1] A. Beniah Ndraha et al., "Analisis Keamanan Data Menggunakan Kriptografi," *Jurnal Teknologi Informasi*, vol. 5, no. 1, 2024.

[2] Marudin and Windarto, "Implementasi Steganografi Least Significant Bit (LSB) Pada Aplikasi Berbasis Desktop Di Pengembang Properti BSA Land," *SKANIKA*, vol. 4, no. 2, pp. 133-138, 2021.

[3] S. N. Nugraha, "Penerapan Algoritma Kriptografi ElGamal Pada Aplikasi Pengamanan Pesan

Berbasis Website," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 12, no. 3, pp. 2523-2531,2024.

[4] E. Y. Hidayat and K. Hastuti, "Analisis Steganografi Metode Least Significant Bit (LSB) dengan Penyisipan Sekuensial dan Acak Secara Kuantitatif dan Visual," *Techno.COM*, vol. 12, no. 3, pp. 157-167, 2013.

[5] Achmad Fauzi, "ANALISA kombinasi pesan teks ke dalam file audio memanfaatkan algoritma data encryption standard dan metode end of file," *J. Tek. Inform. Kaputama*, vol. 1, 2025 .

[6] R. I. H. Nasution, A. Fauzi, dan H. Khair, "Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image," *Journal of Artificial Intelligence and Engineering Applications*, vol. 2, no. 3, 2023.