Jurnal Elektronik Ilmu Komputer Udayana
Volume 15, No 1. August 2026

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Analisis Komparasi Pengamanan Kunci Pemulihan *Wallet Cryptocurrency* Menggunakan Metode LSB *Random* dan *Randomized Adaptive Edge-Based Steganography*

Raihan Akbar Maulana[a1], I Wayan Santiyasa[a2], Ida Ayu Gde Suwiprabayanti Putra[a3], I Wayan Supriana[a4]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, Jimbaran, Kuta Selatan, Badung, Bali, Indonesia

[1]raihanakbarmaulana29@email.com
[2]santiyasa@unud.ac.id
[3]iagsuwiprabayantiputra@unud.ac.id
[4]wayan.supriana@unud.ac.id

Abstrak

Keamanan dompet aset kripto *non-custodial* sangat bergantung pada kerahasiaan 12 kata Kunci Pemulihan (*Recovery Key*). Kegagalan penyimpanan frasa ini pada medium yang rentan memicu risiko peretasan dan kehilangan aset secara permanen. Penelitian ini bertujuan merumuskan arsitektur *cold-storage* alternatif dengan menyembunyikan 132-bit Kunci Pemulihan standar BIP39 ke dalam citra digital guna meningkatkan ketahanannya terhadap serangan siber. Studi komparatif dilakukan untuk memetakan titik batas kegagalan (*breaking point*) dari dua metode steganografi, yaitu *Least Significant Bit* (LSB) Random dan *Randomized Adaptive Edge-Based*. Pengujian dilakukan melalui *stress test* terhadap manipulasi resolusi, pencahayaan, kontras, serta analisis statistik. Hasil evaluasi menunjukkan kedua metode berhasil menyisipkan data tanpa merusak visual citra secara kasatmata. Metode *Edge-Based* unggul pada kualitas struktural (SSIM 0,999992), efisiensi komputasi (0,022 detik), dan keamanan statistik *Chi-Square* (*P-Value* 0,7428). Namun, saat citra mengalami degradasi kontras dan kecerahan ekstrem, metode LSB Random justru lebih tangguh dengan nilai PSNR yang stabil pada kisaran 82 dB. Temuan ini menghasilkan rekomendasi protokol keamanan adaptif: *Edge-Based* sebagai arsitektur utama untuk citra berkualitas tinggi, dan LSB Random sebagai protokol cadangan (*resilient fallback*) pada media berkualitas rendah.

Kata Kunci: *Cryptocurrency, Frasa Pemulihan Wallet, Steganografi, LSB Random, Adaptive Edge-Based, Chi-Square Attack*

1. Pendahuluan

Teknologi *blockchain* yang berkembang pesat mendorong penggunaan *cryptocurrency* sebagai infrastruktur finansial terdesentralisasi [1]. Sebagian besar investor aset digital memilih dompet non-kustodial agar memegang otoritas penuh atas asetnya. Dalam ekosistem ini, kepemilikan dana direpresentasikan oleh Kunci Pemulihan (*Wallet Recovery Phrase*) atau *Seed Phrase*, yang umumnya berupa 12 kata acak sesuai protokol BIP39 [2]. Kerumitan matematis frasa ini membuatnya sangat sulit diretas melalui metode tebakan acak (*brute-force*), namun risiko terbesar justru datang dari kebiasaan penyimpanan pengguna yang tidak aman [3].

Berdasarkan laporan global Chainalysis, kompromi dompet pribadi menyumbang kerugian materiil terbesar dalam industri kripto [4]. Medium penyimpanan fisik seperti kertas, atau data teks tak terenkripsi di perangkat digital, menjadi target utama *malware* [5]. Steganografi dapat memitigasi celah ini. Berbeda dengan kriptografi yang mengacak pesan menjadi teks tidak terbaca, steganografi menyembunyikan eksistensi data (*security through obscurity*) di dalam media penampung seperti gambar, sehingga informasi rahasia tidak memancing kecurigaan pihak mana pun [6].

Least Significant Bit (LSB) merupakan salah satu pendekatan steganografi yang paling sering digunakan karena mampu menyisipkan pesan pada bit terakhir nilai piksel tanpa menimbulkan degradasi warna yang kasat mata [7]. Namun, penyisipan LSB sekuensial (berurutan) konvensional

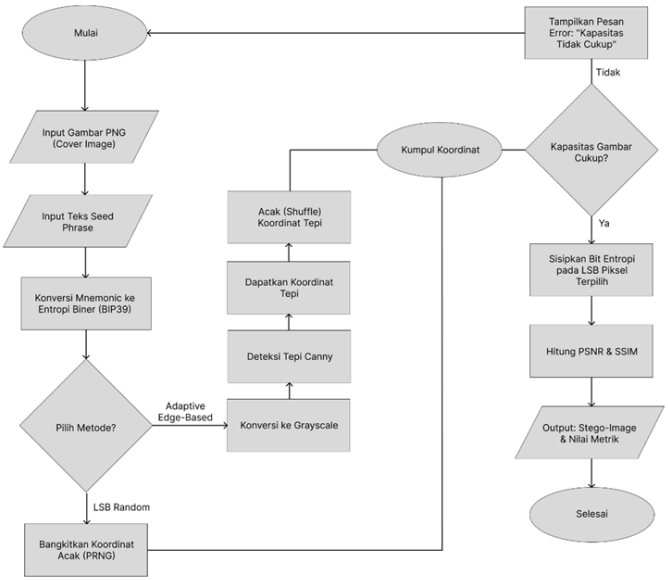
memiliki kelemahan struktural karena mudah dideteksi oleh analisis anomali statistik [8]. Untuk mengatasi kelemahan ini, penelitian ini membandingkan dua pendekatan modifikasi steganografi tingkat lanjut.

Metode pertama, LSB *Random*, mereduksi kelemahan pola sekuensial dengan meratakan sebaran titik koordinat penyisipan menggunakan *Pseudo-Random Number Generator* (PRNG) [9]. Metode kedua, *Randomized Adaptive Edge-Based Steganography*, menyisipkan data secara adaptif: bukan disebar secara acak buta, melainkan difokuskan pada batas tepi (*edges*) objek citra yang bertekstur rumit dengan bantuan algoritma deteksi Canny [10]. Pemanfaatan area kontur ini meminimalkan distorsi visual melalui fenomena penyamaran tekstur (*texture masking*) [11]. Penelitian ini mengukur dan membandingkan performa kedua algoritma terhadap stabilitas kualitas citra, ketahanan pada manipulasi skala ekstrem, beban waktu komputasi, dan ketahanan terhadap evaluasi analitik *Chi-Square Attack* [12, 13].

Meskipun metode LSB dan deteksi tepi telah banyak dieksplorasi, penelitian terdahulu umumnya berfokus pada penyisipan data umum (teks/citra) berkapasitas besar [6, 9]. Penelitian ini memanfaatkan steganografi untuk kasus keamanan yang lebih spesifik dan belum banyak dibahas, yaitu pengamanan data *cryptocurrency* berukuran mikroskopis (132-bit Kunci Pemulihan BIP39) sebagai alternatif arsitektur *cold-storage* (penyimpanan luring) yang lebih tahan terhadap peretasan siber [2, 8]. Selain membandingkan metode LSB *Random* dan *Randomized Adaptive Edge-Based*, penulis juga mengevaluasi titik batas kegagalan operasional (*breaking point*) kedua algoritma tersebut saat citra penampung mengalami degradasi ekstrem [7, 9]. Hasil evaluasi ini digunakan untuk merumuskan rekomendasi metode steganografi yang paling aman dan relevan untuk diadopsi oleh pengembang dompet kripto non-kustodial, berdasarkan kualitas media penyimpanan yang digunakan [2, 7, 10].

2. Metode Penelitian

Alur implementasi dalam riset ini meliputi prapemrosesan data teks, pemrosesan citra, komputasi penyisipan data, serta tahap evaluasi matematis secara otomatis.



Gambar 1. Alur Arsitektur Sistem (Proses *Encoding*)

2.1. Dataset dan Prapemrosesan

Dataset media penampung terdiri dari 24 citra digital *lossless* berekstensi PNG dari *Kodak True Color Image Suite*, yang mewakili keberagaman aspek pencahayaan dan kerapatan garis batas objek. Data rahasia yang diuji berupa 12 kata frasa mnemonik standar BIP39.

Untuk menjaga efisiensi ruang penyisipan, sistem sengaja tidak menggunakan enkripsi karakter berbasis ASCII (8-bit per karakter teks). Sebagai gantinya, sistem mencocokkan setiap kata ke indeks kamus publik BIP39 yang berisi 2048 daftar kata, lalu mengonversi setiap indeks numerik (0 hingga 2047) menjadi nilai biner presisi 11-bit. Melalui binarisasi indeks ini, ukuran total muatan (*payload*) dari

p-ISSN: 2301-5373
e-ISSN: 2654-5101

12 kata dapat dipadatkan menjadi hanya 132-bit (12 kata × 11 bit) sebelum disisipkan ke dalam matriks citra [2].

2.2. Implementasi LSB Random

Pada metode ini, citra penampung dieksekusi secara merata sebagai matriks spasial. *Seed key* (kata sandi) milik pengguna dimanfaatkan untuk membangkitkan koordinat penyisipan acak dari fungsi *Pseudo-Random Number Generator* (PRNG). Masing-masing dari 132 bit pesan yang telah diproses sebelumnya akan menyubstitusi nilai bit terakhir dari kanal warna Biru (B) pada koordinat yang dihasilkan, tanpa memperhitungkan kompleksitas tekstur piksel di sekelilingnya.

2.3. Implementasi *Randomized Adaptive Edge-Based*

Pendekatan adaptif ini bekerja pada domain tekstural: citra pertama-tama diubah ke format skala keabuan (*grayscale*) untuk menjalankan algoritma *Canny Edge Detection* [10]. Ketika sistem mendeteksi piksel di area tepi (*edges*) yang jumlahnya cukup atau melebihi kapasitas 132-bit, urutan koordinat piksel target tersebut diacak menggunakan PRNG. 132 bit Kunci Pemulihan kemudian dikodekan pada kanal warna Biru di titik-titik tepi tersebut, sehingga modifikasi piksel yang terjadi melebur dengan derau warna alami gambar (*texture masking*).

2.4. Skenario Desain Evaluasi

Sistem komparasi dievaluasi menggunakan prototipe perangkat lunak berbasis bahasa pemrograman Python yang menghitung matriks kualitas pengujian berikut:

a. *Imperceptibility*: Diukur secara terintegrasi menggunakan metrik *Peak Signal-to-Noise Ratio* (PSNR) dan *Structural Similarity Index Measure* (SSIM).
b. *Robustness* (Kecerahan): Menguji ketahanan fungsional algoritma saat gambar penampung direduksi atau dipertegas intensitas cahayanya sebelum proses penyisipan.
c. *Robustness* (Kontras): Mengevaluasi imunitas sistem terhadap kepudaran gambar yang secara ekstrem menurunkan tingkat gradien warna objek.
d. *Runtime Efficiency*: Menghitung komparasi rasio beban waktu komputasi (detik) berdasarkan penambahan volume karakter dari *seed key*.
e. *Security*: Menjalankan tes kerentanan analisis distribusi statistik pasif menggunakan perumusan probabilistik *Chi-Square Attack*.

3. Hasil dan Pembahasan

3.1. Analisis Kualitas Visual (Uji Resolusi)

Evaluasi ini digunakan untuk memetakan jumlah kerugian visual yang ditimbulkan dari modifikasi *stego-image*. Pengujian diiterasikan pada skala terkecil (64x64) hingga 1024x1024 piksel.

Tabel 1. Perbandingan PSNR dan SSIM berdasarkan Resolusi Citra

Resolusi	PSNR LSB (dB)	SSIM LSB	PSNR Edge (dB)	SSIM Edge
64x64	70.91	0.999981	70.99	0.999992
256x256	82.99	0.999998	82.82	0.999999
512x512	89.03	0.999999	88.91	1.000000
1024x1024	94.96	1.000000	94.92	1.000000

Data pada Tabel 1 menunjukkan bahwa kapasitas pesan yang mikroskopis (132-bit) membuat rasio pertukaran piksel menjadi tidak signifikan. Seluruh pengujian mencatatkan skor PSNR jauh di atas standar aman 40 dB [7]. Meski demikian, metode *Edge-Based* unggul pada tingkat persepsi manusia: nilai SSIM-nya selalu lebih tinggi atau mencapai rasio 1.000000, yang menunjukkan bahwa penyisipan pada area tepian berhasil menyembunyikan perubahan matematis tanpa merusak struktur kontur utama gambar.

3.2. Analisis Ketahanan Manipulasi Kecerahan (*Brightness*)

Pengujian *stress test* pada tahap pra-penyisipan ini dirancang khusus untuk memetakan kondisi batas kelemahan (*blind spot*) algoritma. Pengujian pertama menurunkan dan menaikkan level intensitas pencahayaan mutlak gambar.

Tabel 2. Dampak Manipulasi Kecerahan Terhadap Kualitas Penyisipan

Faktor Pengali	PSNR LSB (dB)	PSNR Edge (dB)	SSIM LSB	SSIM Edge
0.2 (Sangat Gelap)	82.93	34.55	0.999996	0.416666
1.0 (Normal)	82.99	82.82	0.999998	0.999999
2.0 (Sangat Terang)	82.91	82.84	0.999998	1.000000

Pada Tabel 2, penggelapan ekstrem di skala 0.2 menurunkan nilai pengujian *Edge-Based* hingga 34,55 dB. Penurunan ini bukan disebabkan oleh kesalahan penyisipan data, melainkan oleh kegagalan sensor Canny mendeteksi kontur objek pada gambar yang terlalu gelap, sehingga target ruang 132 piksel tidak dapat dipenuhi. Sebaliknya, metode *LSB Random* mempertahankan nilai PSNR di kisaran ~82 dB karena tidak bergantung pada pembacaan sensor cahaya.

3.3. Analisis Ketahanan Manipulasi Kontras (*Contrast*)

Skenario selanjutnya dalam *stress test* adalah memanipulasi ketajaman *gradient magnitude* antarwarna. Saat skala kontras ditekan hingga 0.2, batas objek akan menyatu dan citra berubah menjadi pudar layaknya hamparan warna abu-abu.

Tabel 3. Dampak Manipulasi Kontras Terhadap Kualitas Penyisipan

Faktor Pengali	PSNR LSB (dB)	PSNR Edge (dB)	SSIM LSB	SSIM Edge
0.2 (Sangat Pudar)	83.08	31.13	0.999996	0.375000
1.0 (Normal)	82.99	82.82	0.999998	0.999999
2.0 (Sangat Tajam)	82.86	82.85	0.999998	0.999999

Tabel 3 kembali memvalidasi titik henti algoritma tekstural. Pemudaran kontras di skala 0.2 merenggut fitur garis pemisah pada gambar, menyebabkan detektor Canny mengalami disorientasi penangkapan piksel tepi, sehingga nilai PSNR *Edge-Based* anjlok ke level 31,13 dB. *LSB Random* tidak terpengaruh oleh gradien kontras dan tetap sukses menyebar bit data dengan nilai PSNR 83,08 dB.

3.4. Kinerja Waktu Komputasi

Metrik durasi dieksekusi dengan mendinamisasi jumlah karakter *password* (PRNG *Seed*) hingga 1000 karakter pada matriks resolusi 512x512.

Tabel 4. Komparasi Waktu Eksekusi Berdasarkan Panjang Karakter Kunci

Panjang Seed Key	Waktu LSB (detik)	Waktu Edge (detik)
10 Karakter	0.106	0.020
500 Karakter	0.110	0.022
1000 Karakter	0.107	0.034

Meski panjang kata sandi bertambah, beban RAM tidak berfluktuasi. Algoritma *Edge-Based* mencatatkan proses hingga lima kali lebih cepat. Perbedaan ini dipicu oleh cara pengacakan koordinat: *LSB Random* memaksa komputer memindai seluruh populasi piksel gambar (262.144 indeks), sementara metode berbasis tepi membatasi iterasi PRNG hanya pada koordinat yang tervalidasi sebagai tepi, sehingga penggunaan memori menjadi lebih efisien.

3.5. Analisis Keamanan Steganalisis (*Chi-Square*)

Keamanan pasif diukur menggunakan nilai probabilistik distribusi ekuilibrium kurva frekuensi (*Pairs of Values*) pada lapisan bit terakhir (LSB).

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Tabel 5. Hasil Steganalisis Distribusi *Chi-Square*

Algoritma	Rata-rata P-Value	Ambang Signifikansi	Kesimpulan
LSB Random	0.7022	> 0.05	Aman
Edge-Based	0.7428	> 0.05	Aman

Kedua mekanisme steganografi berhasil melewati fase pemindaian karena meraih *P-Value* yang jauh dari zona rawan 0,05 [12]. Meski demikian, keunggulan *Edge-Based* dengan nilai probabilistik 0,7428 menunjukkan bahwa modifikasi data yang bertumpuk pada garis kerumitan tepi objek lebih menyerupai derau intrinsik gambar (*natural noise*) bagi mesin analisis statistik, dibandingkan dengan pengacakan buta *LSB Random* (0,7022) [13].

4. Kesimpulan

Berdasarkan evaluasi komparatif, penelitian ini merumuskan protokol arsitektur *cold-storage* berbasis steganografi yang adaptif terhadap karakteristik media penyimpanan. Model *Randomized Adaptive Edge-Based* ditetapkan sebagai arsitektur primer untuk pengamanan Kunci Pemulihan *Wallet* pada media citra berkualitas tinggi, karena mampu memberikan proteksi superior terhadap deteksi statistik (*P-Value* 0,7428) dan integritas struktural visual (SSIM 0,999992). Sebaliknya, *LSB Random* diformulasikan sebagai protokol cadangan (*resilient fallback*) untuk menangani skenario penyimpanan luring pada media citra dengan kualitas pencahayaan atau resolusi rendah, di mana algoritma deteksi tepi konvensional sering mengalami kegagalan operasional. Temuan ini memberikan landasan empiris bagi pengembang dompet kripto non-kustodial untuk mengintegrasikan mekanisme steganografi yang bersifat *self-adaptive*, di mana pemilihan algoritma penyisipan dapat dilakukan secara otomatis berdasarkan profil tekstur dan kecerahan media penyimpanan pengguna, guna meningkatkan keamanan penyimpanan aset digital pengguna.

Referensi

[1] K. Harahap, T. Anggraini, dan Asmuni, "Cryptocurrency dalam Perspektif Syariah: Sebagai Mata Uang atau Aset Komoditas," NIAGAWAN, vol. 11, no. 1, 2022.

[2] M. Palatinus, P. Rusnak, A. Voisine, dan S. Bowe, "Mnemonic code for generating deterministic keys (BIP39)," Bitcoin Improvement Proposals, 2013.

[3] S. T. Bukhari, M. U. Janjua, dan J. Qadir, "Secure Storage of Crypto Wallet Seed Phrase Using ECC and Splitting Technique," IEEE Open Journal of the Computer Society, vol. 5, pp. 278-289, 2024.

[4] Chainalysis, The 2022 Crypto Crime Report, Chainalysis, 2022.

[5] Federal Bureau of Investigation, 2024 Cryptocurrency Fraud Report, Internet Crime Complaint Center, 2024.

[6] M. A. Firdaus dan A. Rahmatulloh, "Implementasi Steganografi Citra Digital LSB Menggunakan Enkripsi AES-256 dan Embedding Pseudorandom," Jurnal Informatika Dan Teknik Elektro Terapan, vol. 13, no. 1, 2025.

[7] F. Yanti dan K. Budayawan, "Implementasi Metode LSB untuk Penyisipan Pesan pada Citra Digital," Jurnal Vocational Teknik Elektronika Dan Informatika, vol. 11, no. 1, 2023.

[8] A. Westfeld dan A. Pfitzmann, "Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools," Proceedings of the 3rd International Information Hiding Workshop, 1999.

[9] S. Aryasanti, R. Ujiandari, M. Hardjianto, dan R. Kusumawardani, "Implementasi Keamanan File Menggunakan Metode Kriptografi Base-64 dan Steganografi Least Significant Bit (LSB) Random 2-Bit Berbasis Web," TICOM, vol. 11, no. 2, pp. 113-118, 2023.

[10] J. Canny, "A Computational Approach to Edge Detection," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 8, no. 6, pp. 679-698, 1986.

[11] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 2, pp. 104-114, 2022.

[12] R. J. Maulidina, N. B. Idris, dan Djumhadi, "Implementasi Steganografi dan Steganalisis Menggunakan Metode LSB pada File Gambar," Journal Forensic Business Information Systems, 2024.

[13] N. Rokhman dan J. Maharanti, "Deteksi Steganografi Berbasis Least Significant Bit (LSB) Dengan Menggunakan Analisis Statistik," Indonesian Journal of Computing and Cybernetics Systems, vol. 5, no. 1, pp. 57-62, 2011.