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

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

Pendekatan Berbasis GLCM untuk Optimasi Citra Sampul pada Steganografi LSB dengan Keamanan RSA-2048

Gede Eka Putra Wijaya[a1], I Gusti Agung Gede Arya Kadyanan[a2], I Ketut Gede Suhartana [a3]

[a]Program Studi Informatika, Universitas Udayana
Badung, Indonesia

[1]wijayaaputraaaa@gmail.com
[2]gungde@unud.ac.id
[3]ikg.suhartana@unud.ac.id

Abstract

Least Significant Bit (LSB) steganography usually treats every image as an equally good carrier, ignoring that cover texture governs how visible and how detectable the embedded payload becomes. This work proposes a Gray-Level Co-occurrence Matrix (GLCM) approach to rank traditional Indonesian fabric motifs as covers, with the secret first encrypted under RSA-2048 with OAEP padding. Four Haralick features were extracted from 165 grayscale images across 15 motifs, then each image carried multi-bit LSB payloads over a full 3x3 factorial of bit modes and load percentages, yielding 1,485 stego images. Pearson correlation links each feature to quality (MSE, PSNR, SSIM) and to detectability under Chi-square Attack and RS Analysis. Homogeneity is the single strongest predictor, tracking SSIM (r = -0.763 to -0.846) and the RS Gap (r = 0.668 to 0.878), whereas PSNR and MSE capture no texture effect. RS Analysis separates stego from cover far more sharply than Chi-square (AUC 0.986 to 1.000 versus 0.788 to 0.939). A min-max composite score ranks Bali Barong first (0.9394); the worst-case RS Gap between best and worst motif differs by 84.5 percent, confirming that cover choice materially affects security.

Keywords: *LSB steganography, RSA, GLCM, SSIM, Traditional textile, Cover image selection*

1. Pendahuluan

Steganografi merupakan teknik menyembunyikan keberadaan pesan di dalam suatu media, berbeda dengan kriptografi yang hanya membuat isi pesan tidak terbaca. Keduanya sering dikombinasikan. Pesan dienkripsi terlebih dahulu, kemudian ciphertext disisipkan ke dalam media, sehingga menambah lapisan keamanan. Pada citra digital, metode penyisipan yang paling umum digunakan adalah Least Significant Bit (LSB), yaitu dengan mengganti bit paling tidak signifikan pada setiap piksel dengan bit pesan [1]. Metode ini dikenal efisien secara komputasi dan memiliki kapasitas penyisipan yang relatif besar. Namun, metode LSB memiliki kelemahan pada aspek statistik. Proses penyisipan dapat mengubah distribusi pasangan nilai piksel yang bertetangga, sehingga meninggalkan jejak yang dapat dideteksi. Westfeld dan Pfitzmann mengembangkan Chi-square Attack untuk menguji pemerataan pasangan histogram [2], sedangkan Fridrich dkk. memperkenalkan RS Analysis yang mendeteksi gangguan pada struktur kelompok piksel [3]. Kedua metode tersebut banyak digunakan sebagai acuan dalam mengevaluasi ketahanan teknik steganografi.

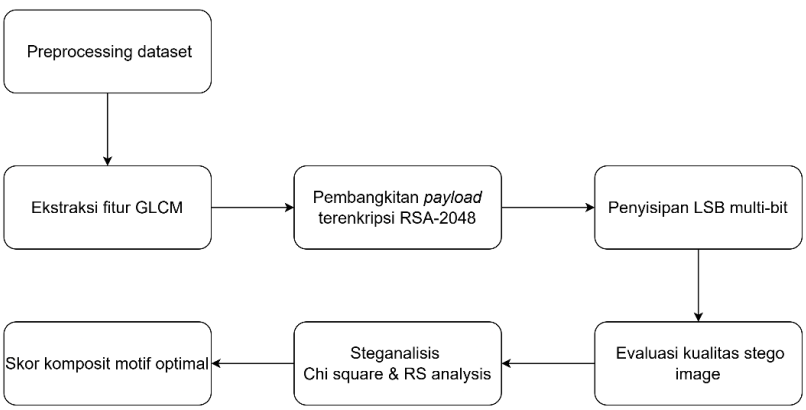
Pemilihan citra sampul merupakan salah satu aspek yang sering kurang diperhatikan dalam penerapan LSB. Banyak pendekatan mengasumsikan bahwa semua citra memiliki kualitas yang setara sebagai media penyisipan, padahal karakteristik citra sangat memengaruhi tingkat detektabilitas. Secara konseptual, citra dengan tekstur kompleks memiliki variasi lokal yang tinggi, sehingga perubahan kecil akibat penyisipan cenderung tersamarkan, sedangkan citra dengan area homogen lebih mudah menunjukkan perubahan tersebut. Penelitian terdahulu tentang pemilihan sampul dapat dikelompokkan menjadi tiga arah. Kelompok pertama memakai

fitur tekstur secara langsung, seperti Subhedar dan Mankar yang menyeleksi sampul berdasarkan fitur termasuk GLCM untuk meningkatkan ketahanan terhadap deteksi [4]. Kelompok kedua memformulasikan pemilihan sampul sebagai persoalan optimasi metaheuristik, seperti Shyla dkk. yang memakai algoritma genetika untuk mencari sampul dengan detektabilitas terendah [5]. Kelompok ketiga memanfaatkan pembelajaran mesin, khususnya *convolutional* neural network, yang secara otomatis memilih wilayah atau citra sampul terbaik melalui proses pelatihan [6], [7]. Ketiga arah tersebut efektif menekan detektabilitas, tetapi memiliki keterbatasan yang sama. Pendekatan berbasis tekstur memperlakukan fitur sebagai kotak hitam tanpa menjelaskan fitur mana yang menentukan, pencarian metaheuristik menuntut iterasi yang mahal secara komputasi, dan pendekatan pembelajaran mesin memerlukan data latih besar serta menghasilkan model yang sulit ditafsirkan.

Berbeda dengan lainnya, penelitian ini mengkaji dan menjelaskan secara kuantitatif fitur GLCM mana yang menentukan kualitas dan ketahanan citra *stego*. Perbedaan utamanya terletak pada transparansi. Hubungan antara tiap fitur tekstur dan hasil steganografi diukur langsung, sehingga dasar pemilihan sampul dapat dijelaskan, bukan sekadar dihasilkan oleh proses yang tertutup. *Gray Level Co-occurrence* Matrix (GLCM) yang diperkenalkan oleh Haralick dkk. merupakan metode untuk mengekstraksi karakteristik tekstur berdasarkan frekuensi kemunculan pasangan intensitas piksel yang bertetangga [8]. Empat fitur turunan yang umum digunakan adalah *Contrast, Correlation, Energy,* dan *Homogeneity*. Dalam konteks batik, GLCM telah banyak dimanfaatkan untuk membedakan motif. Azhar dan Akbi memanfaatkan GLCM untuk temu-kembali citra batik dengan menambahkan fitur *dissimilarity* dan *homogeneity* guna meningkatkan presisi [9]. Sejumlah penelitian lain pada klasifikasi motif daerah juga menunjukkan hasil serupa, termasuk klasifikasi berbasis k-Nearest Neighbor pada jenis batik tertentu [10]. Namun, sebagian besar penelitian tersebut masih berfokus pada klasifikasi, dan belum mengkaji keterkaitan antara fitur GLCM dan performa steganografi secara kuantitatif. Celah inilah yang diisi penelitian ini. Motif kain tradisional Indonesia layak diuji karena rentang teksturnya lebar. Parang Solo bergaris rapat, Megamendung berupa gelombang lembut, dan motif Papua penuh isian padat. Perbedaan ini seharusnya tercermin pada fitur GLCM dan, jika hipotesis pemilihan sampul benar, maka ikut menentukan seberapa aman citra stego yang dihasilkan. Untuk memperkuat keamanan, pesan dienkripsi lebih dulu dengan RSA-2048 skema OAEP sebelum disisipkan, sehingga yang disisipkan adalah ciphertext yang tampak acak [11].

2. Metode Penelitian

Penelitian ini dilaksanakan melalui tujuh tahap yang disusun secara berurutan, sebagaimana ditunjukkan pada Gambar 1, yaitu prapemrosesan citra, ekstraksi fitur GLCM, pembangkitan kunci dan enkripsi RSA, penyisipan LSB, evaluasi kualitas, steganalisis, serta perhitungan skor komposit. Tahap ekstraksi GLCM dilakukan sebelum proses enkripsi karena fitur yang dihasilkan bertujuan untuk merepresentasikan karakteristik citra sampul secara murni, tanpa dipengaruhi oleh proses penyisipan. Sementara itu, kunci RSA dibangkitkan satu kali di awal dan digunakan secara konsisten pada seluruh skenario pengujian guna menjaga keseragaman hasil.



Gambar 1. Alur Metode Penelitian

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

2.1. Dataset dan Preprocessing

Dataset yang digunakan dalam penelitian ini bersumber dari dataset publik Batik Nusantara. Ini merupakan dataset yang dikurasi oleh Hendry HB dan dipublikasikan melalui platform Kaggle (https://www.kaggle.com/datasets/hendryhb/batik-nusantara-batik-indonesia-dataset). Dataset asli tersebut memuat 800 citra batik yang terbagi dalam 20 kelas motif dari berbagai daerah di Indonesia. Dari dataset asli tersebut, dilakukan proses seleksi sehingga hanya 15 kelas motif yang dipertahankan dengan masing-masing kelas terdiri 165 citra motif kain tradisional Indonesia yang mencakup 15 motif dari berbagai daerah, masing-masing diwakili oleh 11 citra. Motif yang digunakan meliputi Aceh Pintu Aceh, Bali Barong, DKI Ondel-Ondel, Jawa Barat Megamendung, Jawa Timur Pring, Lampung Gajah, Madura Mataketeran, Maluku Pala, NTB Lumbung, Papua Asmat, Papua Cendrawasih, Papua Tifa, Solo Parang, Sumatera Barat Rumah Minang, dan Yogyakarta Kawung. Pemilihan motif mempertimbangkan keberagaman geografis dan keragaman karakteristik tekstur visual untuk memastikan representativitas analisis.

Tabel 1. *Sample* data sebelum dan setelah *preprocessing*

Data Raw	Data Proccessed
	

Tabel 1 menunjukkan perbedaan citra sebelum dan sesudah *preprocessing. s*eluruh citra distandarisasi melalui tiga tahap, yaitu *center crop* 80% dari dimensi asli untuk menghilangkan tepi yang tidak representatif, *resize* ke resolusi seragam 512×512 piksel menggunakan interpolasi *Lanczos*, dan konversi ke format *grayscale* PNG 8-bit. Standarisasi ini memastikan perbandingan yang adil antar motif dan konsistensi perhitungan metrik kualitas.

2.2. Ekstraksi Fitur Tekstur GLCM

Citra dikuantisasi dari 256 ke 16 level keabuan untuk mengurangi kompleksitas. Matriks dihitung berdasarkan empat sudut 0°, 45°, 90°, 135° pada jarak d = 1 dan d = 2, selanjutnya disimetrisasi serta dinormalisasi menjadi probabilitas P(i,j). Empat fitur Haralick dihitung melalui Persamaan (1) sampai (4), dan nilai empat sudut dirata-rata agar fitur tidak bergantung orientasi.

$$Contrast = \sum_{i,j} (i-j)^2 P(i,j) \tag{1}$$

$$Correlation = \frac{\sum_{i,j} (i-\mu_x)(j-\mu_y) P(i,j)}{\sigma_x \sigma_y} \tag{2}$$

$$Energy = \sum_{i,j} P(i,j)^2 \tag{3}$$

$$Homogeneity = \sum_{i,j} \frac{P(i,j)}{1 + |\, i - j \,|} \tag{4}$$

2.3. Pembangkitan *Payload* Terenkripsi RSA-2048

Pesan rahasia dienkripsi menggunakan RSA-2048 dengan *padding* OAEP (SHA-256) sebelum disisipkan ke dalam citra. Kapasitas *plaintext* per blok RSA adalah 190 byte, di hitung dari $k - 2 \cdot hLen - 2 = 256 - 64 - 2 = 190$. Untuk setiap skenario, kapasitas *payload* aktual dihitung sebagai berikut

$$C_{max} = \frac{W \times H \times n}{8} \text{ byte,}$$
$$P_{actual} = \left\lfloor \frac{C_{max} \times \rho}{256} \right\rfloor \times 256 \tag{5}$$

di mana n adalah mode bit, ρ adalah persentase *payload*, dan pembulatan ke kelipatan 256 byte menyesuaikan dengan ukuran blok RSA. Selanjutnya, dilakukan pembangkitan *plainteks* acak yang disesuaikan dengan ukuran target *payload* pada setiap skenario. *Plainteks* ini kemudian dienkripsi menggunakan algoritma RSA-2048 sehingga menghasilkan *ciphertext* dengan panjang yang konsisten per blok, dan total ukurannya tepat memenuhi kapasitas *payload* yang telah ditentukan pada masing-masing skenario.

2.4. Penyisipan LSB Multi-bit

Penyisipan dilakukan secara sekuensial dari piksel pertama. Setiap piksel dimodifikasi menggunakan operasi *bitwise*.

$$piksel_{baru} = (piksel_{asli} \ AND \ mask) \ OR \ bit_{pesan} \tag{6}$$

dengan masker 0xFE (1-bit), 0xFC (2-bit), dan 0xF8 (3-bit). *Header* 4-byte yang menyimpan panjang pesan disisipkan terlebih dahulu untuk memungkinkan ekstraksi yang akurat pada sisi penerima. Operasi lengkapnya ditunjukkan pada tabel 2 berikut.

Tabel 2. Pseudocode Penyisipan LSB Multi-bit

```
1:  procedure SISIP_LSB(citra, pesan, n)        // n = 1,2,3
2:      header ← PANJANG(pesan) sebagai 4 byte
3:      bit ← KE_BIT(header + pesan)
4:      mask ← 256 - 2^n                        // kosongkan n LSB
5:      flat ← RATAKAN(citra)
6:      idx ← 0
7:      for k ← 0 to PANJANG(bit) step n do
8:          v ← NILAI_DESIMAL(bit[k : k+n])
9:          flat[idx] ← (flat[idx] AND mask) OR v
10:         idx ← idx + 1
11:     end for
12:     return BENTUK_ULANG(flat, ukuran citra)
13: end procedure
```

2.5. Evaluasi Kualitas *Stego Image*

Kualitas *stego image* dievaluasi menggunakan tiga metrik komplementer, dengan SSIM mengikuti kerangka penilaian kualitas citra oleh Wang dkk. [12], sebagai berikut.

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i,j) - K(i,j)]^2 \tag{7}$$

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

$$PSNR = 10log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (8)$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (9)$$

2.6. Pengujian Steganalisis Statistik

Dua metode steganalisis digunakan dengan *threshold* objektif berbasis distribusi *cover* dengan aturan 3-sigma τ = μ + 3σ. *Chi-Square Attack* mendeteksi anomali *Pair-of-Values* (PoV) pada histogram dengan persamaan berikut.

$$\chi^2 = \sum_k \frac{(y_{2k} - y_k^*)^2}{y_k^*}, y_k^* = \frac{y_{2k} + y_{2k+1}}{2} \quad (10)$$

Sedangkan *RS Analysis* mengukur divergensi distribusi *regular - singular* pada blok 1×4 piksel dengan persamaan berikut.

$$RS_{gap} = |\ (R_M - S_M) - (R_{-M} - S_{-M})\ | \quad (11)$$

Threshold ditetapkan dari 165 citra *cover*: τ_chi = 0,2564 (μ = 0,0110, σ = 0,0818) dan τ_rs = 2,275% (μ = 0,4727%, σ = 0,6008%). Performa detektor dievaluasi menggunakan TPR, FPR, dan AUC.

2.7. Analisis Korelasi dan Skor Komposit

Korelasi Pearson dihitung antara fitur GLCM dengan agregasi *rotation-invariant* pada d = 1 dan metrik kualitas (PSNR, SSIM, MSE). Uji signifikansi menggunakan uji-t dengan derajat bebas df = n − 2 dan ambang batas p < 0,05.

$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2 \cdot \sum(Y_i - \bar{Y})^2}} \quad (12)$$

Untuk memilih motif terbaik, tiga komponen dinormalisasi min-max lalu dirata-rata dengan bobot sama dan dihitung dengan persamaan berikut.

$$Skor = \frac{SSIM_n + Chi_n + (1 - RSGap_n)}{3} \quad (13)$$

Ketiga komponen dinormalisasi min-max terlebih dahulu agar berada pada skala 0 sampai 1 sebelum digabungkan, sehingga tidak ada komponen yang mendominasi akibat perbedaan satuan atau rentang nilai. Bobot seragam sebesar sepertiga dipilih karena penelitian ini tidak mengasumsikan preferensi tertentu di antara ketiga kriteria. Imperseptibilitas yang diwakili SSIM, ketahanan terhadap Chi-square Attack, dan ketahanan terhadap RS Analysis dipandang sama penting dalam konteks pemilihan sampul yang aman.

3. Hasil dan Pembahsan

3.1. Profil Fitur GLCM Antar Motif

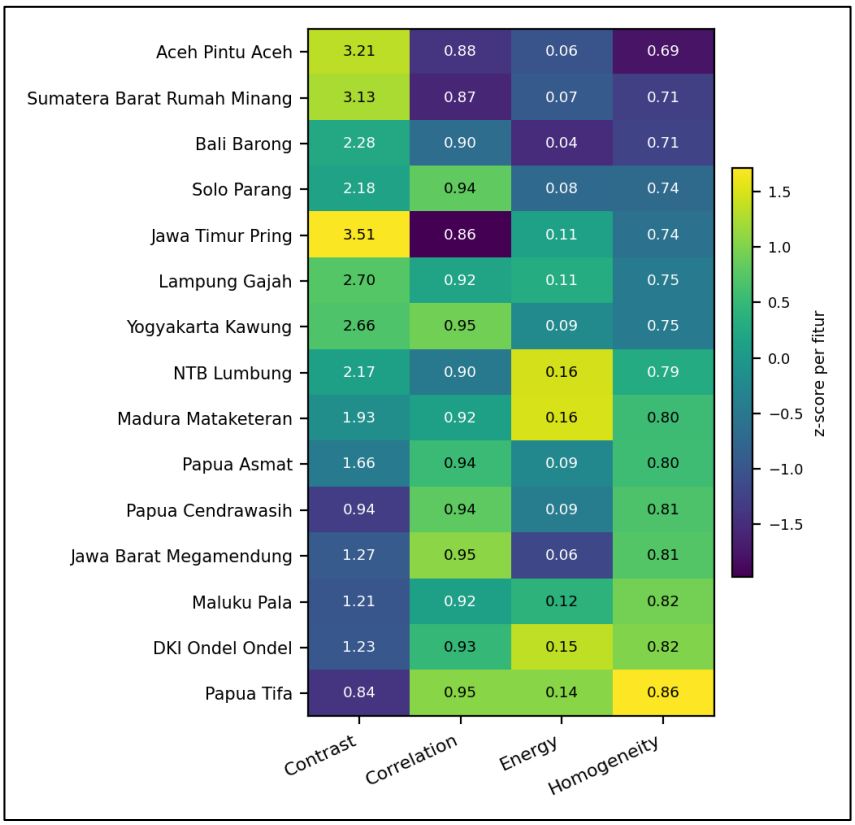
Ekstraksi fitur GLCM pada 165 citra cover menghasilkan profil tekstur yang beragam antar motif. *Contrast* memiliki keragaman terbesar dengan koefisien variasi 82,5 persen, sedangkan

Correlation paling stabil dengan 6,1 persen.

Tabel 3. Statistik deskriptif fitur GLCM pada 165 citra (d = 1)

Fitur	Rata-rata	Min	Maks	CV (%)
Contrast	2,0597	0,2013	9,4152	82,5
Correlation	0,9193	0,6301	0,9870	6,1
Energy	0,1020	0,0141	0,4257	72,7
Homogeneity	0,7737	0,5387	0,9122	10,3

Gambar 2 memetakan keempat fitur untuk 15 motif dalam bentuk *heatmap* dengan normalisasi z-score per kolom, diurutkan dari nilai *Homogeneity* terendah hingga tertinggi. Gradien pola tampak konsisten dan terstruktur. Motif dengan *Homogeneity* tinggi, seperti Papua Tifa dan Maluku Pala, berkorelasi dengan Contrast yang rendah serta Energy yang tinggi. Sebaliknya, motif dengan pola garis teratur seperti Aceh Pintu Aceh berada pada ekstrem berlawanan, yaitu *Homogeneity* rendah, *Contrast* tinggi, dan Energy rendah. Visualisasi ini memperjelas distribusi statistik antar motif dan memberikan representasi konkret terhadap nilai koefisien variasi sebesar 82,5 persen.



Gambar 2. *Heatmap* karakterisasi dataset: 15 motif terhadap empat fitur GLCM

3.2. Korelasi GLCM dengan Kualitas Citra Stego

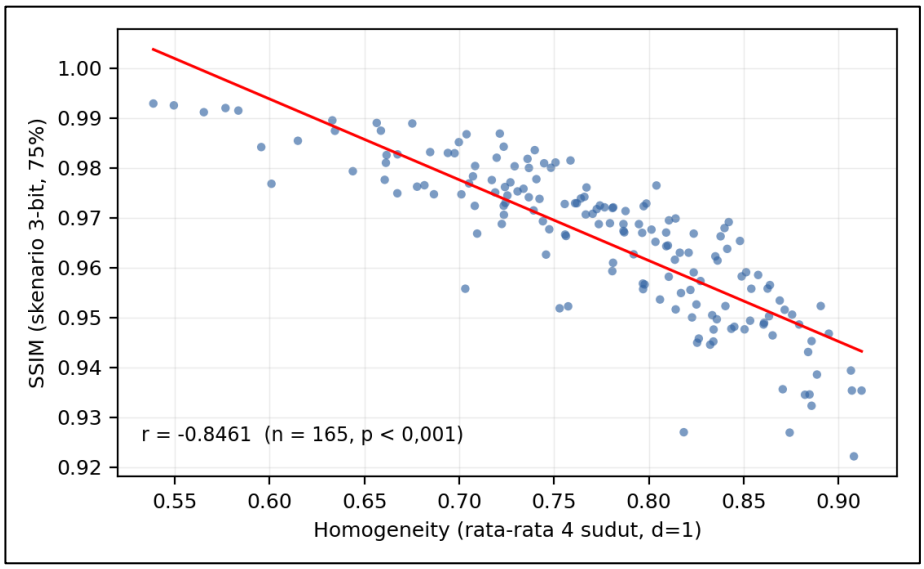
Hasilnya memperlihatkan dikotomi tajam. Keempat fitur GLCM berkorelasi kuat dan signifikan dengan SSIM, tetapi tidak berkorelasi dengan PSNR maupun MSE. *Homogeneity* menjadi

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

prediktor SSIM terkuat, dari -0,763 pada skenario ringan sampai -0,846 pada skenario terberat. Berikut merupakan *sample* hasil dari beberapa skenario korelasi.

Skenario	vs SSIM	vs PSNR	vs MSE
S1 (1-bit, 25%)	-0,7716*	-0,0771	+0,0772
S5 (2-bit, 50%)	-0,8074*	+0,0455	-0,0408
S9 (3-bit, 75%)	-0,8461*	+0,0070	+0,0003

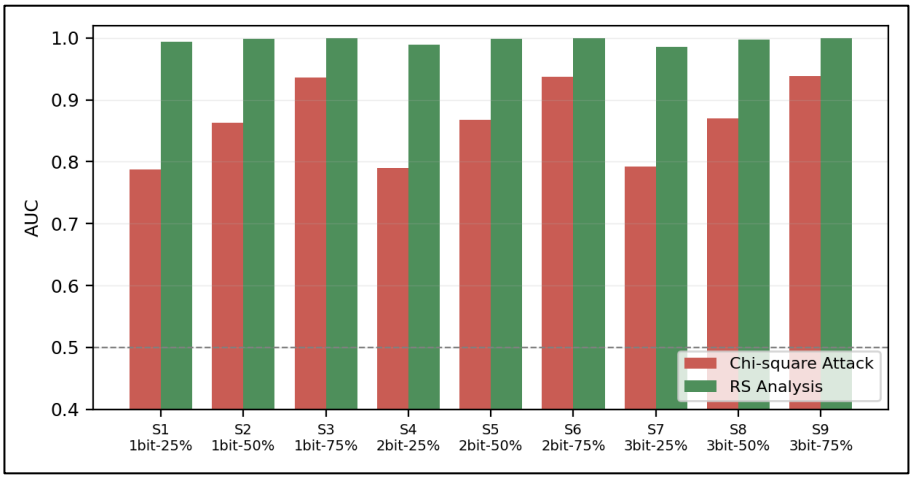
Tanda korelasi negatif menunjukkan bahwa semakin homogen suatu citra sampul, semakin besar penurunan nilai SSIM setelah penyisipan. Hal ini terjadi karena area dengan keabuan yang seragam memiliki variasi struktural yang rendah, sehingga perubahan kecil pada bit LSB langsung memengaruhi kesamaan struktural. Sebaliknya, citra dengan tekstur kompleks mampu menyerap perubahan yang sama tanpa menghasilkan penurunan SSIM yang signifikan. Gambar 3 menampilkan sebaran *Homogeneity* terhadap SSIM pada skenario terberat.



Gambar 3. Sebaran *Homogeneity* terhadap SSIM pada skenario S9 (r = -0,846)

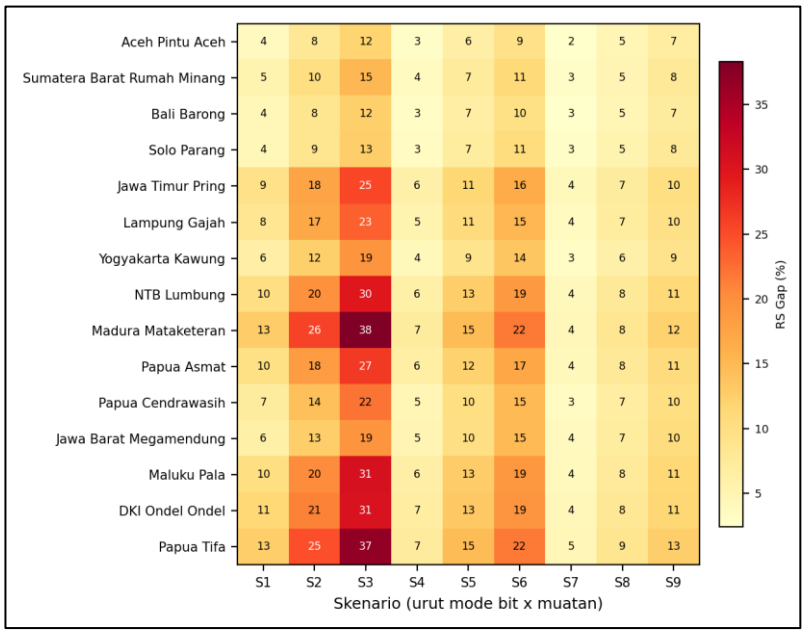
3.3. Steganalisis dan Korelasi dengan Detektabilitas

RS Analysis secara konsisten mengungguli Chi-square Attack pada seluruh sembilan skenario. Nilai AUC RS Analysis berada pada rentang 0,986 hingga 1,000, sedangkan Chi-square hanya mencapai 0,788 hingga 0,939. Secara agregat, *RS Analysis* mampu mengidentifikasi 96% citra *stego*, jauh melampaui *Chi-square* yang hanya mencapai 34%. Performa *Chi-square* baru mendekati andal pada muatan tinggi, sementara pada muatan rendah tingkat deteksinya turun di bawah 11%. Sebaliknya, *RS Analysis* tetap mempertahankan tingkat deteksi di atas 83% bahkan pada kondisi muatan rendah.



Gambar 4. Perbandingan AUC *Chi-square Attack* dan *RS Analysis* per skenario

Distribusi ketahanan antar motif dan skenario ditunjukkan pada Gambar 5 melalui *heatmap* RS Gap untuk 15 motif terhadap sembilan skenario, yang diurutkan berdasarkan nilai *Homogeneity*. Gradien vertikal memperlihatkan pola yang konsisten yaitu motif dengan *Homogeneity* tinggi menghasilkan RS Gap yang lebih besar, sehingga lebih mudah dideteksi. Sementara itu, gradien horizontal menunjukkan peningkatan RS Gap seiring dengan bertambahnya mode bit dan persentase muatan.



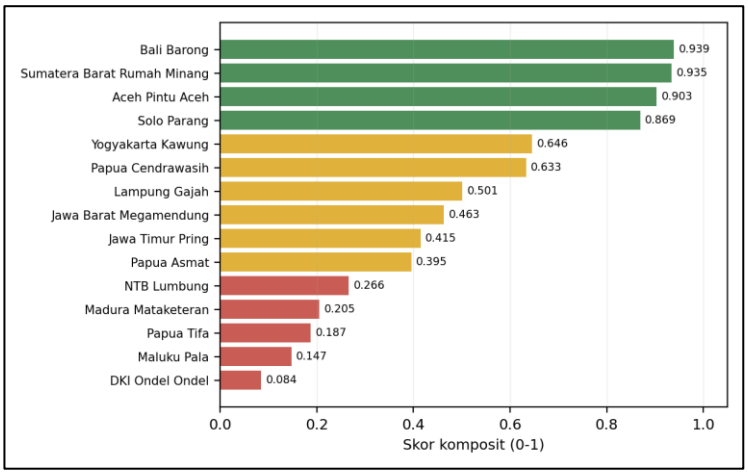
Gambar 5. *Heatmap* RS Gap 15 motif terhadap sembilan skenario

Analisis korelasi memperkuat temuan tersebut. *Homogeneity* kembali menjadi prediktor paling dominan, kali ini terhadap RS Gap dengan korelasi positif berkisar antara r = 0,668 hingga 0,878. Arah korelasi ini melengkapi hasil pada sisi kualitas, citra yang lebih homogen tidak hanya mengalami penurunan SSIM yang lebih besar, tetapi juga menghasilkan jejak statistik yang lebih kuat terhadap deteksi RS. Dengan demikian, *homogeneity* secara simultan mampu memprediksi dua aspek krusial dalam steganografi, yaitu degradasi kualitas visual dan tingkat detektabilitas.

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

3.4. Skor Komposit dan Motif Optimal

Skor komposit menggabungkan SSIM rata-rata, p-value *Chi-square* rata-rata, dan invers RS Gap S9. Bali Barong menempati peringkat pertama dengan skor 0,9394, diikuti Sumatera Barat Rumah Minang 0,9346 dan Aceh Pintu Aceh 0,9032. DKI Ondel-Ondel menempati posisi terakhir 0,0844. Peringkat lengkap divisualkan pada Gambar 6.



Gambar 6. Skor komposit 15 motif

Selisih RS Gap antara motif terbaik dan terburuk pada kondisi terberat mencapai 84,5 persen relatif. Angka ini menjawab pertanyaan pokok penelitian. Memilih Bali Barong alih-alih Papua Tifa menurunkan jejak yang dibaca *RS Analysis* hampir separuh, tanpa mengubah algoritma penyisipan sedikit pun.

4. Kesimpulan

Fitur tekstur GLCM pada motif kain tradisional terbukti efektif untuk memandu pemilihan citra sampul dalam steganografi LSB yang diamankan dengan RSA-2048. Di antara seluruh fitur, *Homogeneity* muncul sebagai prediktor tunggal terkuat, dengan korelasi konsisten terhadap kualitas visual (SSIM, r = −0,763 hingga −0,846) dan detektabilitas (RS Gap, r = 0,668 hingga 0,878). Sebaliknya, PSNR dan MSE tidak mampu menangkap pengaruh tekstur karena sifatnya yang terbatas pada selisih intensitas piksel.

Dari sisi steganalisis, *RS Analysis* menunjukkan kinerja yang jauh lebih unggul *dibandingkan Chi-square Attack*, dengan AUC pada rentang 0,986 hingga 1,000 berbanding 0,788 hingga 0,939. Hal ini menegaskan bahwa evaluasi ketahanan metode LSB sebaiknya mengandalkan *RS Analysis* sebagai indikator utama. Integrasi metrik kualitas dan detektabilitas melalui skor komposit menghasilkan peringkat motif yang jelas, dengan Bali Barong sebagai pilihan paling optimal. Selain itu, selisih RS Gap sebesar 84,5 persen antara motif terbaik dan terburuk menunjukkan bahwa pemilihan citra sampul memiliki dampak signifikan terhadap keamanan steganografi.

Referensi

[1] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "A novel LSB steganography technique using image segmentation," *J. Univers. Comput. Sci.*, vol. 30, no. 3, pp. 308–332, 2024.

[2] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*, LNCS vol. 1768, Berlin: Springer, 2000, pp. 61–76.

[3] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. ACM Workshop Multimedia and Security*, Ottawa, Canada, 2001, pp. 27–30.

[4] M. S. Subhedar and V. H. Mankar, "Cover selection technique for secure transform domain image steganography," *Iran J. Comput. Sci.*, vol. 4, no. 4, pp. 241–252, 2021.

[5] M. Shyla, K. S. Kumar, and R. K. Das, "Image steganography using genetic algorithm for cover image selection and embedding," *Soft Comput. Lett.*, vol. 3, art. 100021, 2021.

[6] V. Himthani, V. S. Dhaka, M. Kaur, et al., "Comparative performance assessment of deep learning based image steganography techniques," *Sci. Rep.*, vol. 12, art. 16895, 2022.

[7] S. I. Nipu, S. Talukder, et al., "Enhanced CNN-DCT steganography: deep learning-based image steganography over cloud," *SN Comput. Sci.*, vol. 5, 2024.

[8] R. M. Haralick, K. Shanmugam, and I. Dinstein, "Textural features for image classification," *IEEE Trans. Syst. Man Cybern.*, vol. SMC-3, no. 6, pp. 610–621, Nov. 1973.

[9] Y. Azhar and D. R. Akbi, "Performance comparison of GLCM features and preprocessing effect on batik image retrieval," *JOIV Int. J. Inform. Vis.*, vol. 8, no. 3, pp. 1339–1343, 2024.

[10] M. Y. Pusadan, F. Mahfud, et al., "Texture analysis and classification of Lontara batik using GLCM and k-nearest neighbor," *IJCCS Indones. J. Comput. Cybern. Syst.*, vol. 10, no. 3, pp. 776–786, 2026.

[11] A. Alanzy, R. Alomrani, B. Alshammari, and A. Almutairi, "Image steganography using LSB and hybrid encryption algorithms," *Appl. Sci.*, vol. 13, no. 21, art. 11771, 2023.

[12] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.