Jurnal EurekaMatika

Journal homepage: https://ejournal-science.upi.edu/jem/index
doi: https://doi.org/10.17509/jem.v14i2.1584

Kombinasi Kriptografi Hill Cipher-CBC dan Steganografi DCT untuk Pengamanan Pesan pada Citra Digital

Giani Alifia, Rini Marwati, dan Isnie Yusnitha*

Program Studi Matematika, FPMIPA, Universitas Pendidikan Indonesia
*Correspondence author: rinimarwati@upi.edu

ABSTRAK

Keamanan data menjadi kebutuhan mendesak dalam pertukaran informasi digital saat ini. Penelitian ini mengusulkan skema pengamanan pesan rahasia melalui kombinasi kriptografi dan steganografi menggunakan Python. Algoritma Hill Cipher dengan mode operasi Cipher Block Chaining (CBC) diterapkan untuk mengenkripsi pesan menjadi cipherteks, yang selanjutnya disembunyikan ke dalam citra digital menggunakan teknik steganografi Discrete Cosine Transform (DCT). Hasil pengujian menunjukkan pesan rahasia berhasil disisipkan tanpa terdeteksi secara visual. Pengukuran kualitas stego-image melalui uji PSNR menghasilkan nilai rata-rata 50 dB untuk berbagai data percobaan, menunjukkan citra output memiliki kualitas baik dan menyerupai cover-image aslinya. Temuan ini membuktikan bahwa integrasi Hill Cipher-CBC dan DCT efektif untuk pengamanan pesan.

© 2026 Kantor Jurnal dan Publikasi UPI

INFORMASI ARTIKEL

Sejarah Artikel:

Diterima 9 Oktober 2026
Direvisi 20 Oktober 2026
Disetujui 21 Oktober 2026
Tersedia online 23 Oktober 2026
Dipublikasikan 23 Oktober 2026

Kata Kunci:
CBC,
DCT,
Hill Cipher,
PSNR

ABSTRACT

Data security has become an urgent necessity in today's digital information exchange. This research proposes a secret message protection scheme through a combination of cryptography and steganography using Python. The Hill Cipher algorithm with Cipher Block Chaining (CBC) mode of operation is applied to encrypt the message into ciphertext, which is subsequently embedded into a digital image using the Discrete Cosine Transform (DCT) steganography technique. The test results show that the secret message was successfully embedded without being visually detectable. Quality measurement of the stego-image through PSNR testing produced values in the range of 50 dB across all trial data, indicating that the output image has good quality and closely resembles the original cover-image. These findings demonstrate that the integration of Hill Cipher-CBC and DCT is effective for message security.

© 2026 Kantor Jurnal dan Publikasi UPI

Keywords:
CBC,
DCT,
Hill Cipher,
PSNR

1. PENDAHULUAN

Memasuki era modern seperti sekarang ini, penggunaan jaringan internet sebagai alat komunikasi semakin meningkat. Operasi bisnis berskala besar hingga kegiatan sehari-hari, seperti menelusuri internet, mengandalkan teknologi informasi sebagai medianya (Ramalinda et al., 2024). Namun dewasa ini, ancaman, seperti hacker, yang membobol kerahasiaan data pribadi individu maupun organisasi semakin banyak bermunculan. Oleh karena itu, dalam pertukaran data dan informasi, keamanan adalah aspek yang sangat penting dan menjadi prioritas bagi banyak orang di seluruh dunia. Urgensi terhadap keamanan informasi ini mendorong pengembangan berbagai metode penyembunyian data, seperti Kriptografi dan Steganografi (Sopian et al., 2025).

Algoritma *Hill Cipher* merupakan algoritma kriptografi kunci simetris yang efektif digunakan untuk merahasiakan pesan menjadi cipherteks. Dengan sifat linearitas pada *Hill Cipher*, yaitu setiap karakter memiliki keterikatan satu sama lain, menyebabkan algoritma ini sangat sulit untuk diretas dengan metode *ciphertext-only attack* (Azizah et al., 2020). Sebaliknya, dekripsi dapat dilakukan dengan cepat apabila matriks kuncinya sudah diketahui (Susanto et al., 2020). Untuk meningkatkan ketahanan terhadap serangan *hacker*, dalam penelitian ini, algoritma *Hill Cipher* perlu digabungkan dengan mode operasi yang dapat memodifikasi pesan menjadi lebih acak, salah satunya adalah CBC (*Cipher Block Chaining*).

CBC adalah mode operasi kriptografi modern yang bekerja pada blok bit pada pesan, berbeda dengan metode klasik yang bekerja pada karakter asli pesannya. Keunggulan utama CBC terletak pada mekanisme umpan balik. Hasil enkripsi satu blok akan digunakan sebagai kunci untuk memproses blok selanjutnya secara berantai, terus menerus hingga blok terakhir. Blok-blok yang saling bergantung ini menghasilkan cipherteks dengan tingkat kompleksitas yang lebih tinggi, sehingga efektif dalam menjamin kerahasiaan (Afsari et al., 2022).

Steganografi adalah teknik penyembunyian data di dalam *cover media* untuk mengecoh pihak ketiga. Tidak seperti kriptografi yang mengacak karakter pada pesan, steganografi menyematkan pesan ke dalam media sehingga pesan yang disembunyikan tidak menarik perhatian pihak ketiga yang tidak memiliki kewenangan (Sujono et al., 2024). Salah satu metode yang sering digunakan untuk menyembunyikan pesan di dalam gambar adalah *Discrete Cosine Transform* (DCT). DCT merupakan metode transformasi yang memetakan sinyal dari domain spasial ke domain frekuensi dasar. Dalam konteks pengolahan citra, DCT mendekonstruksi gambar menjadi rangkaian gelombang sinusoida dengan variasi magnitudo dan frekuensi. DCT menjadi unggul karena kemampuannya dalam memadatkan energi. Sebagian besar informasi visual yang signifikan dipusatkan hanya pada segelintir koefisien DCT, sementara sisanya diabaikan sehingga tidak merusak kualitas citra secara drastis (Mustafa et al., 2019).

Penelitian yang menggabungkan algoritma kriptografi dengan steganografi salah satunya dilakukan oleh Susanto et al. (2020), yang menggabungkan algoritma kriptografi *Hill Cipher* dengan metode steganografi LSB (*Least Significant Bit*). Dari penelitian tersebut diperoleh kesimpulan bahwa waktu komputasi dipengaruhi oleh panjang pesan yang akan disembunyikan dan disisipkan. Waktu yang diperlukan untuk komputasi kombinasi kedua metode tersebut relatif cepat dengan komputasi tercepat adalah 0,648 detik dengan panjang pesan 2000 karakter, sedangkan komputasi paling lambat adalah 4,534 detik dengan panjang pesan 6000 karakter.

Penelitian lain dilakukan oleh Al-magsoosi (2018) yang menganalisis LSB dan DCT sebagai dasar steganografi. Berdasarkan evaluasi menggunakan PSNR (*Peak Signal-to-Noise Ratio*), metode DCT terbukti lebih unggul dibandingkan LSB. Tingginya nilai PSNR pada DCT menunjukkan bahwa teknik ini mampu menghasilkan *stego image* dengan tingkat distorsi visual yang rendah. Meskipun kapasitas penyimpanan data pada DCT lebih kecil dibandingkan LSB, metode ini tetap lebih direkomendasikan karena keunggulannya dalam mempertahankan kualitas *stego image* yang hampir identik dengan *cover image*-nya.

Kriptografi dan steganografi masing-masing dapat menjaga kerahasiaan data secara mandiri, namun dalam implementasinya masih rentan untuk bisa diretas. Berdasarkan permasalahan tersebut, dibutuhkan pendekatan yang lebih tangguh dengan menggabungkan algoritma kriptografi dan steganografi ke dalam satu sistem keamanan (Sujono et al., 2024). Berangkat dari pendekatan tersebut, pada penelitian ini dilakukan penggabungan algoritma kriptografi *Hill Cipher-Cipher Block Chaining* dengan algoritma steganografi *Discrete Cosine Transform* untuk mengamankan pesan teks ke dalam gambar.

2. METODE

Pada mode ini, masukan yang dikenakan algoritma enkripsi adalah XOR dari blok plainteks sekarang dan blok cipherteks sebelumnya, kasus yang sama untuk setiap bloknya. Setiap blok plainteks yang dioperasikan terhubung satu sama lain, secara berurutan, dengan blok sebelumnya. Dalam *Cipher Block Chaining* (CBC), diperlukan *padding* untuk blok terakhir, apabila panjang bitnya tidak sesuai dengan panjang blok yang ditetapkan, sehingga menjadi blok penuh *b* bit (Afsari et al., 2022).

Operasi XOR, dinotasikan dengan simbol $\oplus$, merupakan operasi logika biner yang secara matematis ekuivalen dengan penjumlahan modulo 2. Hasil dari operasi XOR bernilai 1 jika dan hanya jika kedua *input* memiliki nilai bit yang berbeda, dan bernilai 0 jika keduanya bernilai sama. Kondisi-kondisi tersebut dapat ditunjukkan pada Tabel 1 berikut.

Tabel 1. Tabel Kebenaran XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

2.3. *Discrete Cosine Transform*

Metode DCT menjadi fondasi utama dalam standar kompresi populer seperti JPEG karena kemampuannya menghasilkan rasio kompresi yang tinggi dengan degradasi kualitas yang sangat minim dan sulit dideteksi oleh mata manusia. Dengan kata lain, DCT menawarkan efisiensi kompresi tanpa mengorbankan kualitas visual secara signifikan. Oleh karena itu, penelitian ini menjadi sangat relevan untuk menguji efektivitas DCT dalam kompresi citra

digital serta mengevaluasi dampaknya terhadap pengurangan ukuran *file* dan kualitas citra yang dihasilkan (Rengganis et al., 2025).

Pada DCT, *cover-image* yang sudah dipilih dikonversi dari ruang warna RGB menjadi YCbCr dengan rumus berikut (Kareem et al., 2019):

$$Y = 0.257R + 0.504G + 0.098B + 16,$$

$$Cb = -0.148R - 0.291G0.439B + 128,$$

$$Cr = 0.439R - 0.368G - 0.071B + 128.$$

Nilai YCbCr setiap piksel akan berbeda bergantung pada nilai RGB masing-masing pikselnya. Selanjutnya, citra tersebut dibagi menjadi beberapa blok piksel berukuran 8×8. Pada metode DCT ini, untuk mendapatkan nilai koefisiennya, nilai Y yang dikurangi 128 dari YcbCr untuk mempermudah perhitungan. Nilai tersebut kemudian digunakan untuk perhitungan pada rumus berikut (Sheng et al., 2023):

$$F(u,v) = \frac{C(u)C(v)}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} f(i,j) \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)v\pi}{16}\right)$$

dengan:

$F(u,v)$: nilai koefisien frekuensi pada posisi (u,v);
$f(i,j)$: nilai Y pada koordinat (i,j) dalam blok 8×8 yang sudah dilevel shifting;
u,v : indeks frekuensi horizontal dan vertikal dengan $u,v = 0,1,\dots,7$;
i,j : indeks piksel horizontal dan vertikal dengan $i,j = 0,1,\dots,7$; dan
$C(u), C(v)$: faktor normalisasi.

$C(i)$ pada $F(u,v)$ adalah sebagai berikut:

$$C(i) = \{\frac{1}{\sqrt{2}}, \quad \text{jika } i = 0,1, \qquad \text{jika } i > 0.$$

Setelah diperoleh koefisien DCT, nilai tersebut dikuantisasi dengan (Krasmala et al., 2017):

$$F^Q(u,v) = \left[\frac{F(u,v)}{Q(u,v)}\right]$$

dengan $Q(u,v)$ merupakan matriks kuantisasi pada Gambar 1 (Krasmala et al., 2017):

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}.$$

Gambar 1. Matriks Kuantisasi

Kemudian, dilakukan *zig-zag scanning* lalu dipilih nilai koefisien frekuensi tengah karena pada piksel tersebut, penglihatan manusia tidak terlalu sensitif terhadap perubahannya seperti pada frekuensi rendah, dan juga tidak akan terkena dampak perubahan piksel saat kompresi seperti frekuensi tinggi. Pesan yang ingin disisipkan dikoversi menjadi bentuk biner kemudian disubstitusi ke nilai koefisien yang sudah ditentukan.

Selanjutnya, koefisien-koefisien frekuensi dari blok tersebut dikonversi kembali dengan mengalikannya berdasarkan matriks kuantisasi sebelumnya lalu dilakukan invers DCT dengan rumus sebagai berikut:

$$F(i,j) = \frac{1}{4}\sum_{i=0}^{7}\sum_{j=0}^{7} C(u)C(v)f(u,v)\ cos\ cos\left(\frac{(2i+1)u\pi}{16}\right)\ cos\ cos\left(\frac{(2j+1)v\pi}{16}\right)$$

dengan:

$F(i,j)$: nilai *Y* pada koordinat (i,j) dalam blok 8×8;
$f(u,v)$: nilai koefisien frekuensi pada posisi (u,v);
u,v : indeks frekuensi horizontal dan vertikal dengan $u,v = 0,1,\dots,7$;
i,j : indeks piksel horizontal dan vertikal dengan $i,j = 0,1,\dots,7$; dan
$C(u), C(v)$: faktor normalisasi.

Dari nilai yang dihasilkan, perlu ditambah 128 lagi untuk mengembalikan ke nilai *Y*. Sehingga diperoleh kembali gambar, yang kini berisi pesan, dari nilai-nilai piksel tersebut.

2.4. *Peak Signal to Noise Ratio*

Peak Signal to Noise Ratio (PSNR) didefinisikan sebagai metrik perbandingan antara nilai kekuatan sinyal maksimum yang mungkin terhadap kekuatan derau (*noise*) yang mendistorsi sinyal tersebut. Pengukuran ini dinyatakan dalam skala desibel (dB). Dalam konteks pengolahan citra, nilai PSNR berbanding lurus dengan kualitas visual, artinya, semakin tinggi nilai PSNR yang dihasilkan, semakin tinggi pula tingkat kemiripan antara citra hasil pemrosesan (*stego-image*) dengan citra aslinya (*original image*) (Sara et al., 2019).

Untuk membandingkan *stego image* dengan hasil *cover*, diperlukan suatu ukuran kualitas citra. Ukuran yang umum digunakan adalah *Mean-Squared Error* (MSE) dan PSNR. Rumus dari kedua ukuran tersebut ditunjukkan sebagai berikut:

$$PSNR = 10.\log\left(\frac{MAX_I^2}{MSE}\right) = 20.\log\left(\frac{MAX_I}{MSE}\right),$$

dengan

$$MSE = \frac{1}{mn}\sum_{i}^{m}\sum_{j}^{n}\left|I_{(i,j)} - K_{(i,j)}\right|^2,$$

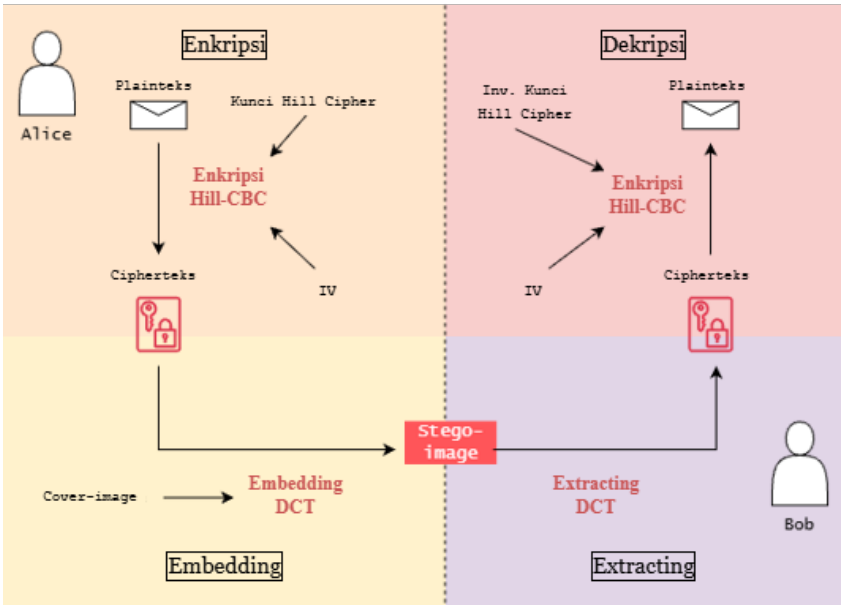
di mana

MAX_i : maksimum nilai *pixel*;
m : panjang citra (dalam *pixel*);
n : lebar citra (dalam *pixel*);
(i,j) : koordinat masing-masing *pixel;*
I : nilai intensitas citra asli; dan
K : nilai intensitas citra setelah disisipi pesan (*stego-image*).

3. HASIL DAN PEMBAHASAN

3.1. Skema Program Pengamanan Pesan dengan Hill-CBC dan DCT

Skema program pengamanan pesan dengan algoritma kriptografi Hill-CBC dan algoritma steganografi DCT ditunjukkan pada Gambar 2 berikut.

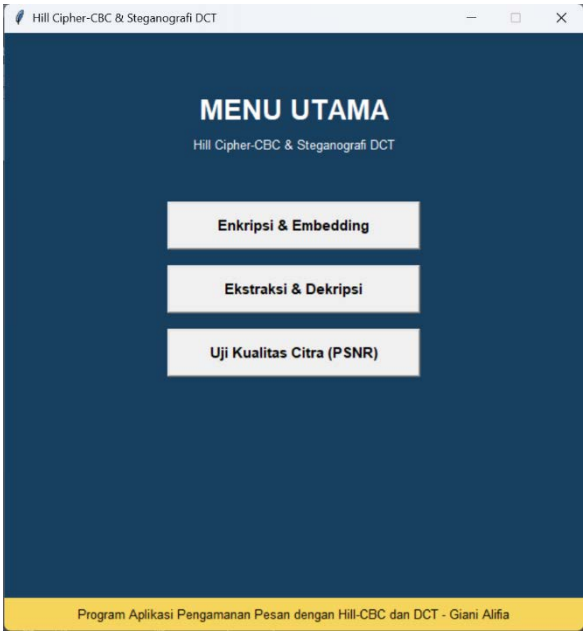


Gambar 2. Skema Program Aplikasi

Alice, sebagai pengirim, menyiapkan pesan rahasia lalu dienkripsikan dengan algoritma Hill-CBC sehingga menghasilkan cipherteks. Kemudian, cipherteks tersebut disisipkan ke dalam *cover-image* agar tersembunyikan. Hasil dari penyisipan tersebut ialah berupa *stego-image* yang kemudian dikirimkan ke Bob bersama dengan kunci *Hill Cipher* dan *Initial Value* (IV). Bob mengekstraksi *stego-image* untuk mendapatkan cipherteks, lalu cipherteks tersebut didekripsi menggunakan kunci dan IV yang telah diberikan Alice sebelumnya sehingga diterimalah pesan rahasia tersebut oleh Bob.

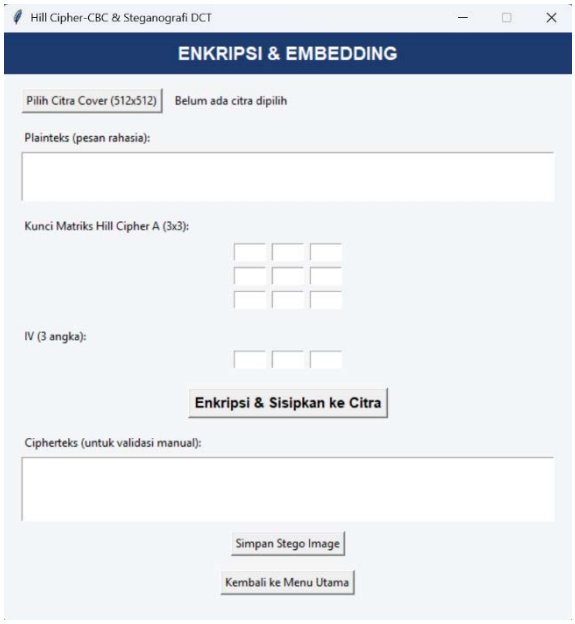
3.2. Tampilan Program Pengamanan Pesan dengan Hill-CBC dan DCT

Pada menu utama terdapat tiga tombol, yaitu Enkripsi-*Embedding*, *Extracting*-Dekripsi, dan Pengujian Citra untuk menuju menu masing-masing. Tampilan dari menu utama pada program ini ditunjukkan pada Gambar 3 berikut.



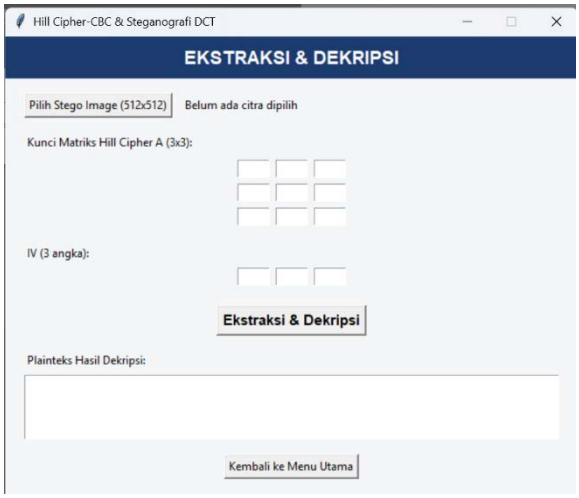
Gambar 3. Tampilan Menu Utama

Tampilan dari menu Enkripsi-*Embedding* ditunjukkan pada Gambar 4 berikut.



Gambar 4. Tampilan Menu Enkripsi-Embedding

Tampilan dari menu *Extracting*-Dekripsi ditunjukkan pada Gambar 5 berikut.



Gambar 5. Tampilan Menu Extracting-Dekripsi

Tampilan dari menu Pengujian Kualitas Citra ditunjukkan pada Gambar 6 berikut.



Gambar 6. Tampilan Menu Pengujian Kualitas Citra

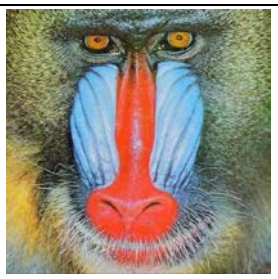
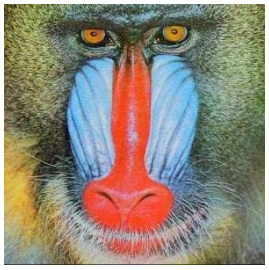
3.2. Validasi Program Pengamanan Pesan dengan Hill-CBC dan DCT

Setelah proses enkripsi dan *embedding* menghasilkan *stego image*, tahap berikutnya adalah pengujian kualitas citra tersebut melalui validasi. Pengujian kualitas ini memanfaatkan metode *Peak Signal to Noise Ratio* (PSNR), yang dirumuskan sebagai $PSNR = 10.log\ log\left(\frac{MAX_I^2}{MSE}\right)$, di mana MAX_I^2 menyatakan nilai piksel tertinggi yang mungkin ada pada citra. Karena penelitian ini menggunakan format citra RGB, maka nilai MAX_I^2 yang dipakai adalah 255. Sementara itu, MSE dihitung dari rata-rata kuadrat selisih piksel antara citra asli (*cover image*) dan citra hasil penyisipan pesan (*stego image*). Proses validasi ini dilakukan dengan mengambil sampel langsung dari keluaran (*output*) aplikasi komputer yang telah dibuat.

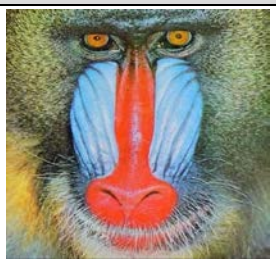
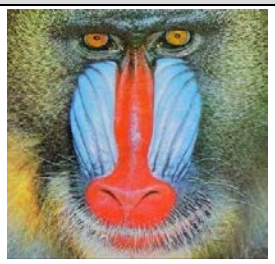
Untuk melihat kualitas hasil *embedding* pada program ini, akan digunakan jenis citra RGB, biner, dan *grayscale*, dan pula beberapa ukuran citra yang berbeda, sebagai *cover-image*. Beberapa panjang plainteks yang berbeda juga akan digunakan untuk melihat kemampuan program dalam menyisipkan pesan. Setelahnya, *stego-image* yang dihasilkan akan diuji kualitasnya menggunakan uji PSNR seperti yang dilakukan pada citra RGB

sebelumnya. Kunci enkripsi, serta IV yang digunakan masih sama seperti citra sebelumnya. Hasil pengujian berbagai jenis citra dan panjang plainteks ditunjukkan pada Tabel 2 berikut.

Tabel 2. Pengujian PSNR pada Berbagai Jenis Citra

No.	Jenis Citra	Ukuran Citra	Panjang Plainteks (karakter)	*Cover-image*	*Stego-image*	Nilai PSNR
1	RGB	720×720	18			61
2	RGB	447×447	18			47
3	RGB	256×256	18			51
4	*Grays cale*	371×499	18			52
5	Biner	256×256	18			45

No.	Jenis Citra	Ukuran Citra	Panjang Plainteks (karakter)	*Cover-image*	*Stego-image*	Nilai PSNR
6	RGB	720 × 720	100			54
7	RGB	447 × 447	100			41
8	RGB	256 × 256	100			44
9	*Grays cale*	371 × 499	100			46
10	Biner	256 × 256	100			37
11	RGB	720 × 720	450			47

No.	Jenis Citra	Ukuran Citra	Panjang Plainteks (karakter)	*Cover-image*	*Stego-image*	Nilai PSNR
12	RGB	447×447	450			35
13	RGB	256×256	450			36

Berdasarkan berbagai percobaan yang ditunjukkan pada Tabel 2, dapat disimpulkan sebagai berikut.

1. Pada plainteks dengan panjang 18 karakter, citra RGB berukuran 720×720 menghasilkan kualitas *stego-image* terbaik dengan nilai PSNR sebesar 61. Sementara itu, citra *grayscale* dan biner sama-sama menghasilkan nilai PSNR yang masih tergolong tinggi.
2. Pada plainteks dengan panjang 100 karakter, citra RGB berukuran 720×720 masih menghasilkan kualitas *stego-image* terbaik namun dengan nilai PSNR yang lebih kecil, yaitu 54. Sementara itu, citra *grayscale* dan biner sama-sama menghasilkan nilai PSNR yang semakin rendah namun masih cukup baik.
3. Terakhir, pada plainteks dengan panjang 450 karakter, citra RGB berukuran 720×720 tetap menghasilkan kualitas *stego-image* terbaik dengan nilai PSNR sebesar 47. Nilai tersebut tentunya semakin rendah karena pesan yang disisipkan semakin panjang. Nilai PSNR pada citra RGB berukuran 447×447 memang lebih rendah dibandingkan ukuran 720×720, namun masih lebih tinggi dibandingkan dengan citra RGB berukuran 256×256.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa pengamanan pesan rahasia melalui kombinasi kriptografi Hill Cipher mode CBC dan steganografi DCT berhasil diterapkan melalui tiga tahapan, proses enkripsi-embedding di sisi pengirim, ekstraksi-dekripsi di sisi penerima, serta pengujian kualitas citra (MSE dan PSNR), yang diimplementasikan dalam bentuk aplikasi desktop berbasis Python dengan GUI. Validasi melalui uji PSNR yang dihasilkan tergolong sangat baik dengan stego-image yang secara visual hampir tidak dapat dibedakan dari cover-image aslinya. Dengan demikian, skema hibrida ini terbukti mampu memberikan perlindungan keamanan ganda, baik dari segi kerahasiaan pesan melalui enkripsi matematis, maupun penyamaran keberadaannya secara visual dalam citra digital.

5. DAFTAR PUSTAKA

Afsari, Mulyana, Damaiyanti, & Sa'adah, 2022. Implementasi mode operasi kombinasi cipher block chaining dan metode LSB-1 pada pengamanan data teks. *Jurnal Pendidikan Sains dan Komputer*, *2*(1), 70 - 82. https://doi.org/10.47709/jpsk.v2i01.1381

Al-magsoosi, 2018. Comparison study between LSB and DCT based steganography. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 20 (1), 47-52. https://doi.org/10.9790/0661-2001014752

Azizah, Marwati, & Yusnitha, 2020. Penggabungan modifikasi hill cipher dan elliptic curve cryptography untuk meningkatkan keamanan pesan. *Jurnal EurekaMatika,* 8(2). https://doi.org/10.17509/jem.v8i2.30743

Kareem, Daway, & Daway, 2019. Underwater image enhancement using colour restoration based on YCbCr colour model. *IOP Conf. Series: Materials Science and Engineering,* 571, 012125. https://doi.org/10.1088/1757-899x/571/1/012125

Krasmala, Purba, & Lenggana, 2017. Kompresi citra dengan menggabungkan metode Discrete Cosine Transform (DCT) dan Algoritma Huffman. *Jurnal Online Informatika*, 2(1). https://doi.org/10.15575/join.v2i1.79

Mustafa, Yazid, Khairunizam, Jamlos, Zunaidi, Razlan, & Shahriman, 2019. Image enhancement based on Discrete Cosine Transforms (DCT) and Discrete Wavelet Transform (DWT): A Review*. IOP Conf. Series: Materials Science and Engineering*, 557, 012027. https://doi.org/10.1088/1757-899x/557/1/012027

Rengganis, Siambaton, & Aulia, 2025. Image compression application using Discrete Cosine Transform (DCT) Method. *Proceeding of International Conference on Science and Technology UISU*, *7929*, 244–250. https://doi.org/10.30743/kvc7ef82

Ramalinda, Jayadi, & Raharja., 2024. Strategi perlindungan data menggunakan sistem kriptografi dalam keamanan informasi. *Journal of International Multidisciplinary Research*, 2(6), 665–671. https://doi.org/10.62504/jimr679

Sara, Akter, & Uddin, 2019. Image quality assessment through FSIM, SSIM, MSE and PSNR—A comparative study. Journal of Computer and Communications, 7(3). https://doi.org/10.4236/jcc.2019.73002

Sheng, Li, Bhatti, Liu, Huang, & Chen, 2023. Zero watermarking algorithm for medical image based on Resnet50-DCT. *Computers, Materials & Continua*, 75(1), 293-309. https://doi.org/10.32604/cmc.2023.036438

Sopian, Fatimah, & Marwati, 2025. Penggunaan fungsi Hitzl-Zele pada implementasi gabungan Secret Sharing Shamir's (t, w)-Threshold Scheme dan steganografi audio Least Significant Bit. *Jurnal EurekaMatika,* 12(1), 1-14. https://doi.org/10.17509/jem.v13i1.74549

Sujono, Marwati, & Kustiawan, 2024. Pengamanan citra grayscale menggunakan penggabungan kriptografi visual Secret Sharing dan Steganografi Enhanced Least Significant Bit. *Jurnal EurekaMatika*, 12(2), 67-78. https://doi.org/10.17509/jem.v12i2.72580

Susanto, Mulyono, Febrian, & Rosyida, 2020. A combination of Hill Cipher and LSB for image security. *Scientific Journal of Informatics*, *7*(1), 155–165. https://doi.org/10.15294/sji.v7i1.24393