Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 12, No. 5, Oktober 2025, hlm. 1115-1122 e-ISSN: 2528-6579

STUDI PENDEKATAN *QUALITY & DIFFERENTIAL ANALYSIS* TERHADAP KINERJA ALGORITMA AES-CBC PADA ENKRIPSI GAMBAR

Sartika Gafur[1], Eko Aribowo[*2]

[1,2]Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
Email:[1]gafursartika@gmail.com, [2*]ekoab@tif.uad.ac.id
*penulis Korespondensi

(Naskah masuk: 12 November 2024, diterima untuk diterbitkan: 30 Oktober 2025)

Abstrak

Penelitian ini mengeksplorasi pendekatan *Quality & Differential Analysis* untuk menilai kinerja algoritma *AES-Cipher Block Chaining (AES-CBC)* pada enkripsi gambar dengan resolusi 512 x 512 piksel. Algoritma AES-CBC dipilih karena kemampuannya menyediakan enkripsi blok yang aman dan efisien terhadap data berstruktur pada gambar berekstensi *.jpg, *.jpeg, *.png, *.gif, *.bmp, *.tiff, *.webp, *.heic, *.heif, *.svg, *.raw, *.psd, dan *.ico. Penelitian ini menggunakan tujuh metrik evaluasi yang komprehensif: *Encryption Quality* (MSE, RMSE, PSNR, SSIM) dan *Differential Analysis* (NPCR, UACI, CC), yang lebih komprehensif dibandingkan beberapa penelitian sebelumnya yang umumnya hanya menggunakan dua atau tiga metrik. Hasil penelitian menunjukkan bahwa algoritma AES-CBC mampu menghasilkan enkripsi gambar yang kuat, dengan nilai MSE dan RMSE sebesar 0.0, PSNR tak terhingga (inf dB), dan SSIM 1.0. Nilai NPCR berkisar antara 99.97% hingga 100%, UACI antara 49.87% hingga 50.26%, dan CC antara -0.0055 hingga 0.007, menunjukkan kemampuan algoritma dalam menangani perubahan diferensial. Penelitian ini memberikan wawasan mendalam tentang efektivitas algoritma AES-CBC dalam mengamankan file gambar dan menawarkan analisis menyeluruh tentang kualitas enkripsi dan ketahanannya terhadap serangan diferensial. Hasil penelitian ini diharapkan dapat berkontribusi pada pengembangan teknik enkripsi yang lebih aman di masa depan.

Kata kunci: *AES-CBC, enkripsi gambar, Quality & Differential Analysis, keamanan data, evaluasi kinerja.*

STUDY OF QUALITY & DIFFERENTIAL ANALYSIS APPROACH TO PERFORMANCE OF AES-CBC ALGORITHM ON IMAGE ENCRYPTION

Abstract

*This research explores Quality & Differential Analysis approach to assess the performance of AES-Cipher Block Chaining (AES-CBC) algorithm on image encryption with 512 x 512 pixels resolution. The AES-CBC algorithm was chosen for its ability to provide secure and efficient block encryption of structured data in images with the extensions *.jpg, *.jpeg, *.png, *.gif, *.bmp, *.tiff, *.webp, *.heic, *.heif, *.svg, *.raw, *.psd, and *.ico. This research uses seven comprehensive evaluation metrics: Encryption Quality (MSE, RMSE, PSNR, SSIM) and Differential Analysis (NPCR, UACI, CC), which is more comprehensive than some previous studies that generally only use two or three metrics. The results show that the AES-CBC algorithm is able to produce strong image encryption, with MSE and RMSE values of 0.0, PSNR infinity (inf dB), and SSIM 1.0. NPCR values range from 99.97% to 100%, UACI between 49.87% to 50.26%, and CC between -0.0055 to 0.007, demonstrating the algorithm's ability to handle differential changes. This research provides an in-depth insight into the effectiveness of the AES-CBC algorithm in securing image files and offers a thorough analysis of its encryption quality and resistance to differential attacks. The results of this research are expected to contribute to the development of more secure encryption techniques in the future.*

Keywords: *AES-CBC, image encryption, Quality & Differential Analysis, data security, performance evaluation.*

1. PENDAHULUAN

Di era digital yang serba terhubung saat ini, data telah menjadi aset yang sangat berharga. Namun, seiring dengan meningkatnya penggunaan teknologi, ancaman pencurian data oleh pihak luar untuk kepentingan pribadi semakin mengkhawatirkan. Keamanan data kini menjadi prioritas utama untuk memastikan kerahasiaan dan keaslian informasi tetap terjaga selama proses berbagi dan transfer. Kriptografi menjadi salah satu solusi utama untuk melindungi data dari akses yang tidak sah, dengan menyembunyikan pesan dan informasi. Berbagai teknik dan algoritma kriptografi, baik yang klasik maupun modern, digunakan untuk menjaga keamanan data yang ditransmisikan melalui jaringan seperti internet (Hidayati, Fitriana and Adam, 2021).

Algoritma kriptografi enkripsi *Advanced Encryption Standard* (AES) diakui dan banyak direkomendasikan. AES adalah algoritma enkripsi kunci simetris yang mendukung panjang kunci bervariasi dan bilangan bulat. Enkripsi menggunakan 10 putaran untuk kunci 128-bit, 12 putaran untuk kunci 192-bit, dan 14 putaran untuk kunci 256-bit. AES dapat digunakan dalam berbagai mode, dan salah satu yang cocok untuk enkripsi gambar adalah mode *Cipher Block Chaining* (CBC) karena menghindari pola yang terlihat, di mana blok gambar yang identik akan menghasilkan blok *ciphertext* yang identik (Alghamdi and Munir, 2024).

Algoritma ini memiliki kemampuan untuk meningkatkan keamanan data dengan cara merantai proses enkripsi setiap blok gambar, memastikan bahwa perubahan kecil pada data asli dapat memengaruhi seluruh hasil enkripsi. Selain itu, menggunakan *Initialization Vector* (IV) yang berbeda di setiap sesi enkripsi meningkatkan keamanan dengan memastikan hasil enkripsi selalu unik, meskipun kunci yang sama digunakan. Ini membantu mencegah penyalahgunaan atau serangan terhadap data (Nurhandhi and Suhendar, 2023). Dalam operasi CBC, mekanisme *feedback* diterapkan pada blok bit, di mana hasil enkripsi blok pertama digunakan sebagai IV untuk blok berikutnya. Proses ini berlanjut hingga semua blok bit habis, menyebabkan setiap blok hasil enkripsi saling bergantung satu sama lain (Mahmud and Mintorini, 2020).

Menilai kualitas metode enkripsi gambar sangat penting untuk memastikan bahwa gambar asli tidak mengalami penyimpangan yang signifikan terhadap proses dekripsi. Untuk menilai kontribusi metode tersebut, metrik evaluasi seperti PSNR dan SSIM sering digunakan. PSNR dipilih karena kemudahan komputasi dan validitasnya dalam berbagai penelitian pemrosesan gambar (Setiadi, 2020). MSE dan RMSE menilai keamanan dan kualitas algoritma enkripsi gambar. Metrik-metrik ini secara bersama-sama memastikan bahwa gambar terenkripsi aman dan gambar yang didekripsi tetap berkualitas tinggi (Gupta and Vijay, 2022; Alexan et al., 2023; Parvathraj and Anoop, 2023).

Selain itu, keacakan hasil enkripsi dievaluasi dengan analisis diferensial menggunakan NPCR, UACI, dan *Correlation Coeficient* (CC) untuk menentukan seberapa efektif algoritma dalam mencegah pola terdeteksi oleh pihak yang tidak berwenang (Hidayati, Fitriana and Adam, 2021).

Penelitian ini bertujuan untuk mengeksplorasi pendekatan *Quality & Differential Analysis* untuk menilai kinerja algoritma *AES-Cipher Block Chaining* (AES-CBC) pada enkripsi gambar.

2. METODE PENELITIAN

Studi sebelumnya telah mengeksplorasi kinerja algoritma enkripsi pada gambar dengan menggunakan berbagai metrik evaluasi.

2.1. *Advanced Encryption Standard – Cipher Blockchaining*

Advanced Encryption Standard (AES) adalah *cipher* blok standar yang menggunakan kunci dan *Initialization Vector*, dan dapat dijalankan dalam berbagai mode, termasuk *Cipher Block Chaining* (CBC) (G, A and S, 2022). AES mengenkripsi data dalam blok 128-bit dan setiap putarannya melibatkan operasi berbasis jaringan substitusi-permutasi (SPN), seperti *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey. Menggunakan* S-box sebagai tabel substitusi yang digunakan dalam proses enkripsi AES dengan mengganti setiap *byte*, yang memiliki efek nonlinieritas tinggi pada proses enkripsi. (Alghamdi and Munir, 2024) .

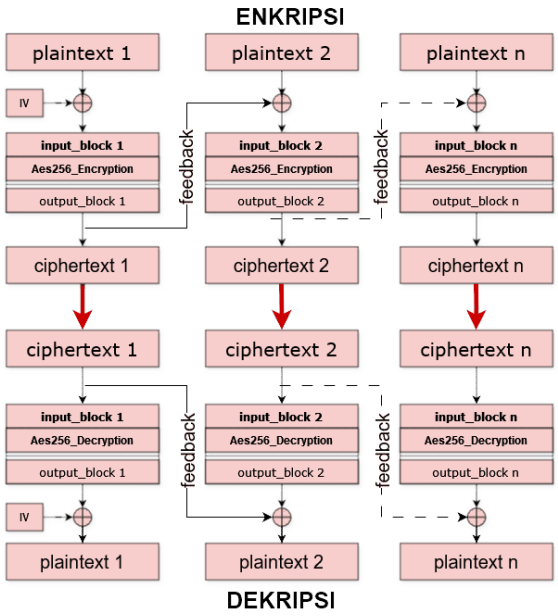
Dalam mode operasi *Cipher Block Chaining* (CBC), S-box menyediakan transformasi nonlinier yang meningkatkan keacakan dan kekuatan kriptografi. Desain CBC menyembunyikan pola berulang dan menciptakan efek persebaran, yang meningkatkan kekuatan kriptografi secara keseluruhan (Alimzhanova, Skublewska-Paszkowska and Nazarbayev, 2023).

Padding mengacu pada proses penambahan byte pada sebuah pesan untuk memastikan bahwa bahwa *plaintext* adalah kelipatan dari ukuran blok yang dibutuhkan oleh algoritma enkripsi, seperti AES-CBC, yang memiliki ukuran blok 16 *byte*. Hal ini diperlukan karena AES beroperasi pada blok dengan ukuran tetap, dan *padding* memungkinkan pesan dengan panjang yang bervariasi untuk dienkripsi dengan benar (Figueroa, 2023).

Cipher Block Chaining (CBC) memulai proses enkripsi dengan menggunakan operasi XOR pada blok pertama *plaintext* bersama IV, menghasilkan blok pertama *ciphertext*. Blok *plaintext* berikutnya di-XOR dengan blok *ciphertext* sebelumnya sebelum dienkripsi. Pada mode ini, hasil enkripsi dari blok sebelumnya digunakan untuk mengenkripsi blok saat ini. Blok *plaintext* saat ini terlebih dahulu di-XOR-

kan *dengan* blok *ciphertext* dari enkripsi sebelumnya.

Alurnya diilustrasikan pada Gambar 1 berikut.



Gambar 1. Alur AES-CBC

Hasil XOR kemudian dienkripsi. Dalam mode CBC, setiap blok *ciphertext* bergantung pada blok *plaintext* saat ini serta seluruh blok *plaintext* sebelumnya (Ismadiah, Syahrizal and Ramadhani, 2020).

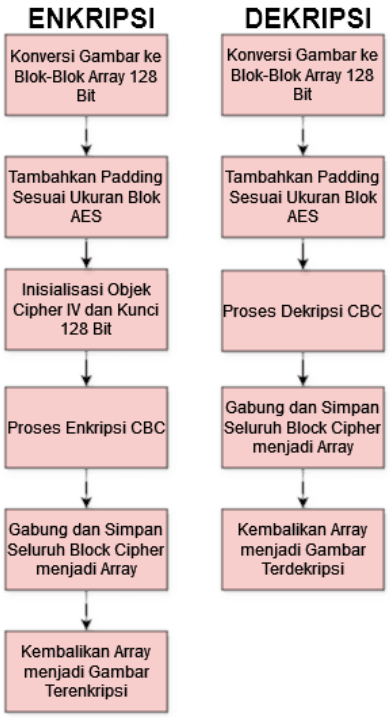
Jika panjang pesan tidak sesuai dengan ukuran blok, blok terakhir diisi dengan *padding*. Pendekatan ini memastikan hasil enkripsi berbeda untuk setiap *plaintext* yang sama, menambah keamanan dan mencegah pola yang mudah dikenali.

Dekripsi dalam mode CBC dilakukan dalam urutan terbalik. Setelah mendekripsi blok terakhir dari *ciphertext*, data yang dihasilkan di-XOR-kan dengan blok *ciphertext* sebelumnya untuk mendapatkan kembali *plaintext*.

2.2. Pembacaan Gambar

Gambar asli dibagi ke dalam blok matriks dan transformasi aritmetik diterapkan. Misalnya, gambar 256 × 256 dibagi menjadi 8 × 8 blok. Dua urutan aritmetika dibuat untuk mengkodekan baris dan kolom matriks, dan matriks 2 × 2 yang baru dibentuk dari elemen diagonal. Gambar diproses melalui serangkaian langkah yang melibatkan pembagian menjadi beberapa bagian, mengekstraksi kunci, dan menerapkan algoritme enkripsi atau dekripsi.

Dalam proses enkripsi, gambar dibagi menjadi empat bagian yang sama, dan kunci diekstraksi dari lima *pixel* pertama setiap baris. Gambar dimanipulasi menggunakan kunci-kunci ini untuk membuat gambar sandi, dan dekripsi melibatkan pembalikan operasi ini menggunakan kunci rahasia untuk mengambil gambar asli (Noshadian, Ebrahimzade and Kazemitabar, 2020; Yan, Wang and Xian, 2021).



Gambar 2. Alur Enkripsi dan Dekripsi Gambar dengan AES-CBC

2.3. Metrik *Encryption Quality*

Hasil gambar kemudian dievaluasi untuk menilai seberapa baik algoritma AES-CBC dalam menjaga integritas dan kualitas gambar dengan membandingkan antara gambar asli (*original*) dan dekripsi.

Metrik MSE (*Mean Squared Error*) mengukur kualitas gambar berdasarkan kesalahan *pixel*, dan digunakan untuk menilai kemiripan gambar (Wang et al., 2021). Dengan cara ini, gambar yang dikompresi tetap mempertahankan kualitas visual yang optimal. Rumus yang dipakai untuk perhitungannya adalah:

$$MSE = \frac{1}{MxN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(I_{ij} - S_{ij}\right)^2 \quad (1)$$

Variabel M dan N merepresentasikan tinggi × lebar dimensi gambar dengan satuan *pixel*, *I(ij)* adalah nilai intensitas *pixel* dalam koordinat *i,j* dari gambar asli. Range nilainya dari 0-14255 untuk gambar 8-bit *grayscale*. *S(ij)* namun menggunakan koordinat *i,j* dari gambar terenkripsi maupun terdekripsi.

Untuk menilai kualitas sebuah gambar, diperlukan nilai RMSE (*Root Mean Squared Error*) yang semakin mendekati nol. Artinya, semakin besar nilai MSE (*Mean Square Error*) dari suatu gambar, semakin besar pula kesalahan yang dihasilkan oleh gambar tersebut (Setiadi, 2020). Perhitungannya menggunakan rumus berikut:

$$RMSE = \sqrt{MSE} \quad (2)$$

Dalam memperkirakan seberapa baik gambar hasil pengolahan dilihat dari sudut pandang manusia dibandingkan dengan gambar asli sebelum pengolahan metrik perbandingan antara gambar asli dan gambar yang dikompresi dalam desibel (Chowdhary et al., 2020), Metrik ini dihitung menggunakan rumus berikut:

$$PSNR = 10.log_{10}\left(\frac{255x255}{MSE}\right) \quad (3)$$

Nilai PSNR (*Peak Signal-to-Noise Rasio*) untuk kompresi gambar bervariasi antara 30-50 dB untuk data 8-bit dan 60-80 dB untuk data 16-bit. Persamaan ini menggambarkan kesalahan absolut dalam dB (Sara, Akter and Uddin, 2019).

Nilai PSNR lebih dari 40 dB (desibel) menandakan rekonstruksi gambar berkualitas tinggi dengan penyimpangan minimal (Geetha et al., 2022). Nilai PSNR lebih tinggi memastikan pemulihan gambar asli secara penuh dan akurat setelah ekstraksi data (Malik et al., 2020), sehingga mengurangi kemungkinan deteksi oleh pihak tidak berwenang (Armijo-Correa et al., 2020).

SSIM (*Structural Similarity Indeks*) memberikan representasi yang lebih akurat tentang kualitas gambar yang dirasakan dibandingkan dengan MSE atau PSNR, karena SSIM bekerja dengan mengevaluasi perubahan pencahayaan, kontras, dan struktur pada bagian lokal gambar, sehingga dianggap lebih tepat dalam mengukur kualitas gambar sesuai persepsi manusia (Reznik, 2023). Untuk menghitung metrik ini, digunakan rumus berikut:

$$SSIM(x,y) = [l(x,y]^{\propto}.[c(x,y]^{\beta}.[s(x,y]^{\gamma} \quad (4)$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)}$$

Fungsi perbandingan pencahayaan *I(X,Y)* untuk gambar asli *X* dan gambar terdekripsi *Y*, Di mana μx dan μy masing-masing adalah nilai rata-rata *X* dan *Y* dan *C1* adalah konstanta stabilisasi dalam proses pengolahan (Sankpal and Vijaya, 2021).

2.4 Metrik *Differential Analysis*

Gambar original dan terenkripsi diukur dan dibandingkan untuk melihat perubahan intensitas antar *pixel* pada gambar. Metrik ini juga penting untuk menentukan keacakan, keamanan, dan kinerja algoritma enkripsi serta memastikan gambar sensitif terlindungi dari akses tidak sah. (Chowdhary et al., 2020).

Algoritma enkripsi yang baik harus sangat sensitif terhadap perubahan kecil pada kunci, sehingga semakin banyak nilai *pixel* yang berubah, semakin bagus kualitas keacakan yang dihasilkan. Analisis akan dilakukan dengan membandingkan antara gambar asli sebelum dilakukan proses apapun dan hasil enkripsinya (Hidayati, Fitriana and Adam, 2021) (Alghamdi and Munir, 2024). Dapat dihitung dengan rumus:

$$\text{NPCR} = \mathcal{N}(\text{C}^1, \text{C}^2) = \sum_{i,j}\frac{D(i,j)}{T} \times 100\% \quad (5)$$

Nilai NPCR (*Number of Pixels Change Rate*) dan UACI (*Unified Average Changing Intensity*) yang mendekati 99,6093% dan 33,4635% dianggap baik (Yan, Wang and Xian, 2021).

UACI mengukur intensitas rata-rata perbedaan antara dua gambar terenkripsi (*C1* dan *C2*). Metrik ini menilai keacakan enkripsi berdasarkan format dan ukuran gambar. UACI yang tinggi menunjukkan resistensi teknik terhadap serangan. Rumus yang dipakai untuk perhitungannya adalah :

$$\text{UACI} = \mathcal{U}\ (\text{C}^1, \text{C}^2) = \sum_{i,j}\frac{|C^1(i,j)-C^2(i,j)|}{F \cdot T} \times 100\% \quad (6)$$

C1 dan *C2* mewakili *pixel* sebelumnya dan sesudahnya, F mewakili jumlah total *pixel*, dan T mewakili jumlah bit yang menggambarkan *pixel* gambar. Nilai NPCR dan UACI untuk gambar skala *grayscale* dan *color* (Singh, Agarwal and Chand, 2019).

Correlation Coefficient (CC) dapat dihitung dengan membandingkan gambar asli dengan gambar yang didekripsi. Nilai yang kuat berkisar dari 0 hingga mendekati 1. Semakin mendekati 0, semakin kuat hubungan yang menunjukkan enkripsi gambar yang lebih baik (Alsaffar et al., 2020).

Gambar terenkripsi dengan CC terendah dianggap sebagai gambar terenkripsi yang paling efektif (Noshadian, Ebrahimzade and Kazemitabar, 2020). Nilai ini dihitung dengan menggunakan rumus berikut:

$$\text{CC} = \frac{\sum x \sum y\ (I_a - \bar{I}_a)(I_b - \bar{I}_b)}{\sqrt{(\sum x \sum y\ (I_a - \bar{I}_a)\ (\sum x \sum y\ I_b - \bar{I}_b)}} \quad (7)$$

Nilai x dan y mewakili nilai tinggi dan lebar, sedangkan $\bar{I}_a$ dan I_a adalah nilai rata-rata intensitas *pixel* dari seluruh gambar dan intensitas individu dari gambar original, lalu $\bar{I}_b$ dan I_b untuk intensitas *pixel* dari seluruh gambar dan intensitas individu dari gambar terenkripsi (Setiadi et al., 2018).

3. HASIL DAN PEMBAHASAN

Tabel 1 berikut menyajikan tahapan enkripsi dan dekripsi AES-CBC terhadap objek gambar dalam bentuk pseudocode.

Gambar 2 mengilustrasikan proses enkripsi pada AES mode CBC (*Cipher Block Chaining*) dengan objek gambar yang melibatkan pembagian gambar menjadi blok-blok kecil. Setiap blok *plaintext* pertama di-XOR dengan sebuah IV acak, kemudian kemudian XOR-kan hasilnya dengan kunci (*key*) yang dimasukkan ketika program dijalankan.

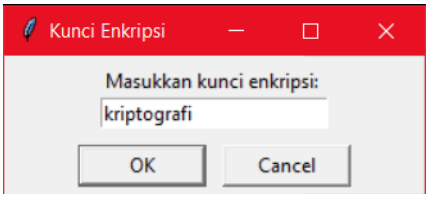
Tabel 1. Pseudocode Alur Enkripsi AES-CBC

Enkripsi AES-CBC	
key_str = AskUser("Enter Encryption Key")	//Meminta pengguna untuk memasukkan kunci enkripsi.
salt = GenerateRandomBytes(16)	//Membuat garam (salt) acak untuk menambah keamanan.
key = PBKDF2HMAC(SHA256, key_str, salt, 390000, 32)	//Mengubah kunci teks menjadi kunci enkripsi menggunakan PBKDF2.
iv = GenerateRandomBytes(AES.block_size)	//Membuat IV (Initialization Vector) acak.
image_bytes = ConvertImageToBytes(image)	//Mengubah gambar menjadi format byte untuk enkripsi.
image_bytes_padded = Pad(image_bytes, AES.block_size)	//Menambahkan padding pada byte gambar agar sesuai blok AES.
cipher = AES(key, AES.MODE_CBC, iv)	//Menginisialisasi algoritma AES dengan mode CBC.
ciphertext = cipher.Encrypt(image_bytes_padded)	//Mengenkripsi byte gambar yang sudah diproses.
ciphertext_array = BytesToNumpyArray(ciphertext)	//Mengubah ciphertext menjadi array NumPy.
expected_size = rows * cols	//Menghitung ukuran yang diharapkan untuk gambar.
if Size(ciphertext_array) < expected_size:	
ciphertext_array = PadToSize(ciphertext_array, expected_size)	
else if Size(ciphertext_array) > expected_size:	
ciphertext_array = TruncateToSize(ciphertext_array, expected_size)	
ciphertext_image = ReshapeArray(ciphertext_array, rows, cols)	//Mengubah array ciphertext menjadi dimensi gambar.

Tabel 2. Pseudocode Enkripsi Alur Dekripsi AES-CBC

Dekripsi AES-CBC	
cipher = AES(key, AES.MODE_CBC, iv)	//Menginisialisasi algoritma AES dengan mode CBC.
plaintext_bytes = cipher.Decrypt(ciphertext)	//Mendekripsi ciphertext untuk mendapatkan byte asli.
plaintext_bytes_unpadded = Unpad(plaintext_bytes, AES.block_size)	//Menghapus padding dari byte hasil dekripsi.
decrypted_image = BytesToNumpyArray(plaintext_bytes_unpadded)	//Mengubah byte hasil dekripsi menjadi array NumPy.
decrypted_image = ReshapeArray(decrypted_image, original_shape)	//Mengembalikan array ke dimensi asli gambar.
if IsGrayscale(decrypted_image):	//Mengecek gambar hasil dekripsi
decrypted_image = ConvertToRGB(decrypted_image)	//Jika grayscale, ubah menjadi format RGB.
else:	//Jika bukan grayscale, lanjut ke langkah berikutnya.
decrypted_image = ConvertToRGB(decrypted_imageDisplayImage(decrypted_image, "Decrypted Image (RGB)")	//Konversi format gambar dari BGR ke RGB. //Menampilkan gambar hasil dekripsi dengan format RGB.

Program implementasi menerima input dalam berbagai karakter sebagaimana yang ditampilkan Gambar 3, kemudian dikonversi ke biner agar sesuai dengan kebutuhan algoritma AES-CBC. Hal ini memungkinkan fleksibilitas dalam penggunaan kunci enkripsi, termasuk huruf, angka, dan tanda baca, yang semuanya dikodekan dalam format UTF-8.



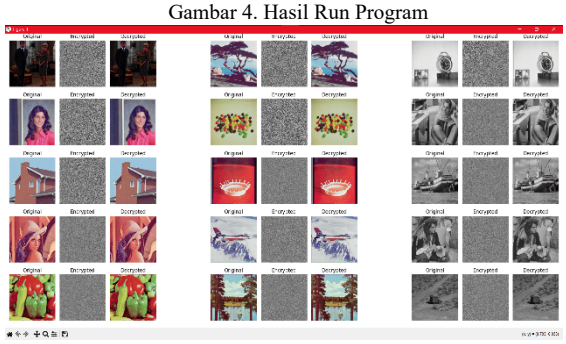
Gambar 3. Jendela untuk Memasukkan Kunci

Berdasarkan program implementasi enkripsi dan dekripsi pada AES mode CBC (*Cipher Block Chaining*) dengan objek gambar dari total 15 dataset *color* dan *grayscale* secara keseluruhan, dihasilkan masing-masing 3 gambar yang meliputi gambar asli, terenkripsi, dan terdekripsi. Program memproses seluruh dataset gamber sekaligus lalu menampilkan hasilnya sebagaimana pada Gambar 4.

Evaluasi metrik menguji performa algoritma AES-CBC (*Cipher Block Chaining*) dalam *Encryption Quality* yang telah diukur menggunakan MSE, RMSE, PSNR, dan SSIM dan *Differential Analysis* yang mencakup NPCR, UACI, dan CC, yang mengukur seberapa sensitif algoritma terhadap perubahan kecil pada data asli.

Key dan *Initialization Vector* yang digunakan, dan hasil perhitungannya masing-masing dicatat pada dua laporan berekstensi *.txt sebagaimana Gambar 5 dan Gambar 6.

Gambar 4. Hasil Run Program



Gambar 5. Laporan yang memuat Key dan IV AES-CBC

Tabel 3 berikut menampilkan nilai *encryption quality* yang memberikan gambaran mendetail tentang kualitas gambar setelah proses enkripsi dan dekripsi menggunakan algoritma AES-CBC.

Tabel 3. Hasil Evaluasi dengan Metrik *Encryption Quality*

Gambar	MSE	RMSE	PSNR	SSIM
Couple.tiff	0.0	0.0	inf dB	1.0

Female.tiff	0.0	0.0	inf dB	1.0
House.tiff	0.0	0.0	inf dB	1.0
Lena.png	0.0	0.0	inf dB	1.0
Pepper.png	0.0	0.0	inf dB	1.0
Tree.tiff	0.0	0.0	inf dB	1.0
JellyBean.tiff	0.0	0.0	inf dB	1.0
Splash.tiff	0.0	0.0	inf dB	1.0
Air Plane.tiff	0.0	0.0	inf dB	1.0
Sailboat.tiff	0.0	0.0	inf dB	1.0
Clock.tiff	0.0	0.0	inf dB	1.0
Boat.tiff	0.0	0.0	inf dB	1.0
Barbara.jpg	0.0	0.0	inf dB	1.0
Pirate.jpg	0.0	0.0	inf dB	1.0
Truck.tiff	0.0	0.0	inf dB	1.0

Semua gambar memiliki nilai MSE dan RMSE sebesar 0.0, yang menunjukkan bahwa tidak ada perbedaan kuadrat rata-rata atau akar kuadrat rata-rata antara gambar asli dan gambar terenkripsi.
Nilai PSNR yang tak terhingga (inf dB) pada semua gambar mengindikasikan bahwa gambar asli dan gambar terenkripsi memiliki sinyal puncak tanpa gangguan, yang menandakan kualitas enkripsi yang sangat tinggi.

Selain itu, nilai SSIM sebesar 1.0 pada semua gambar menunjukkan bahwa struktur gambar asli sepenuhnya dipertahankan dalam gambar terenkripsi, tanpa ada perbedaan struktural.

Secara keseluruhan, analisis ini menunjukkan bahwa algoritma AES mode CBC bekerja dengan sempurna dalam menghasilkan gambar terenkripsi yang sangat mirip dengan gambar asli dalam hal kesamaan struktural dan tidak adanya kesalahan. Hasil ini menegaskan bahwa algoritma AES mode CBC sangat efektif dalam melindungi data gambar secara optimal.

Tabel 4 berikut menampilkan nilai *differential analysis* yang memberikan gambaran mendetail tentang efektivitas enkripsi dalam mengubah *pixel* gambar asli, sehingga memastikan keamanan data yang tinggi menggunakan algoritma AES-CBC.

Tabel 4. Hasil Evaluasi dengan Metrik *Differential Analysis*

Gambar	NPCR	UACI	CC
Couple.tiff	99.98%	49.93%	0.0004
Female.tiff	100.0%	49.97%	0.007
House.tiff	100.0%	50.06%	-0.0043
Lena.png	100.0%	50.0%	-0.0009
Pepper.png	99.98%	49.98%	0.0016
Tree.tiff	100.0%	50.02%	-0.0051
JellyBean.tiff	100.0%	50.26%	0.0026
Splash.tiff	99.99%	49.96%	-0.0013
Air Plane.tiff	100.0%	50.02%	0.0016
Sailboat.tiff	100.0%	49.87%	-0.0055
Clock.tiff	100.0%	50.01%	0.0027
Boat.tiff	100.0%	49.94%	0.0025
Barbara.jpg	100.0%	49.97%	-0.0008
Pirate.jpg	100.0%	50.11%	-0.0002
Truck.tiff	99.99%	49.99%	0.0008

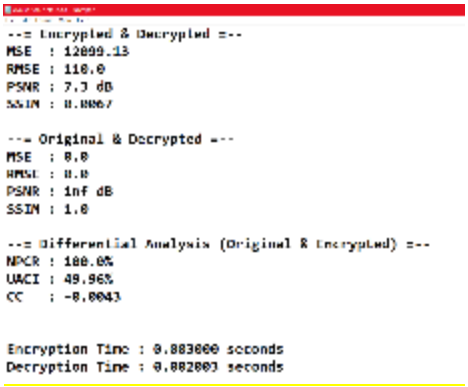
Sebagian besar nilai NPCR berada di kisaran 99.97% hingga 100%, yang menunjukkan bahwa hampir semua *pixel* dalam gambar terenkripsi berubah dibandingkan dengan gambar asli. Nilai ini sangat baik dan menunjukkan bahwa algoritma enkripsi bekerja dengan efektif dalam menghasilkan gambar yang sulit ditebak atau dipecahkan.

Selain itu, nilai UACI berkisar antara 49.87% hingga 50.26%, menyoroti intensitas perubahan *pixel* yang tinggi setelah enkripsi, yang menunjukkan bahwa gambar diacak dengan sangat efektif.

Di sisi lain, nilai CC bervariasi antara -0.0055 hingga 0.007, yang berarti tidak ada korelasi yang signifikan antara gambar asli dan gambar terenkripsi.

Hasil ini menegaskan bahwa enkripsi berhasil menghasilkan gambar terenkripsi yang sangat berbeda dari gambar asli tanpa pola yang dikenali.

Dalam hal kompleksitas waktu pada algoritma AES-CBC, sebagaimana terlampir pada Gambar 6 berikut.



Gambar 6. Kompleksitas Algoritma

Berdasarkan lima kali percobaan yang dilakukan, didapatkan nilai yang ditampilkan pada Tabel 5 berikut.

Tabel 5. Hasil Kompleksitas Waktu Algoritma AES-CBC

Percobaan	Enkripsi	Dekripsi
1	0.003000 sec	0.002003 sec
2	0.004674 sec	0.002046 sec
3	0.006002 sec	0.003999 sec
4	0.003975 sec	0.003517 sec
5	0.001992 sec	0.002011 sec

Dari percobaan tersebut, didapatkan hasil rata-rata untuk enkripsi 0.0039286 detik dan dekripsi 0.0027152.

Secara keseluruhan, analisis ini memperlihatkan bahwa algoritma AES mode CBC memiliki kinerja yang sangat baik dalam melindungi data gambar secara efektif dan acak.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dengan menerapkan Algoritma-CBC (Cipher Block Chaining) pada file gambar dan mengevaluasi kinerjanya, beberapa kesimpulan yang dapat diambil adalah sebagai berikut:

1. Algoritma AES-CBC berhasil diimplementasikan pada file gambar dengan hasil yang menunjukkan perubahan visual

signifikan pada gambar yang terenkripsi. Proses enkripsi dan dekripsi berjalan sesuai dengan yang diharapkan, menjaga integritas data pada gambar yang diolah.

2. Evaluasi kinerja berdasarkan metrik MSE, RMSE, PSNR, dan SSIM menunjukkan bahwa kualitas gambar setelah proses dekripsi sangat mendekati gambar asli. Semua gambar memiliki nilai MSE dan RMSE sebesar 0.0, nilai PSNR yang tak terhingga (inf dB), dan nilai SSIM sebesar 1.0 menunjukkan bahwa Algoritma AES-CBC mampu menjaga kualitas gambar secara optimal setelah proses enkripsi dan dekripsi.
3. Pengujian NPCR dan UACI terhadap algoritma ini memiliki tingkat resistensi yang baik terhadap serangan diferensial. Sebagian besar nilai NPCR berada di kisaran 99.97% hingga 100%, Selain itu, nilai UACI berkisar antara 49.87% hingga 50.26%. Hal ini menunjukkan bahwa AES mode CBC cukup aman dalam menghadapi perubahan kecil pada data input yang dapat mengakibatkan perbedaan besar pada output enkripsi.
4. Hasil pengujian korelasi antar-*pixel* (CC) menunjukkan bahwa AES mode CBC mampu mengurangi korelasi antar-*pixel* pada gambar terenkripsi, nilai CC bervariasi antara -0.0055 hingga 0.007, yang berarti tidak ada korelasi yang signifikan antara gambar asli dan gambar terenkripsi sehingga meningkatkan tingkat keamanan gambar.

DAFTAR PUSTAKA

ALEXAN, W., CHEN, Y.L., POR, L.Y. AND GABR, M., 2023. Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption. Symmetry, 15(5), pp.1–31. https://doi.org/10.3390/sym15051081.

ALGHAMDI, Y. AND MUNIR, A., 2024. Image Encryption Algorithms: A Survey of Design and Evaluation Metrics. Journal of Cybersecurity and Privacy, 4(1), pp.126–152. https://doi.org/10.3390/jcp4010007.

ALIMZHANOVA, Z., SKUBLEWSKA-PASZKOWSKA, M. AND NAZARBAYEV, D., 2023. Periodicity Detection of the Substitution Box in the CBC Mode of Operation: Experiment and Study. IEEE Access, 11(July), pp.75686–75695. https://doi.org/10.1109/ACCESS.2023.3295909.

ALSAFFAR, D.M., SULTAN ALMUTIRI, A., ALQAHTANI, B., ALAMRI, R.M., FAHHAD ALQAHTANI, H., ALQAHTANI, N.N., MOHAMMED ALSHAMMARI, G. AND ALI, A.A., 2020. Image Encryption Based on AES and RSA Algorithms. ICCAIS 2020 - 3rd International Conference on Computer Applications and Information Security, pp.1–5. https://doi.org/10.1109/ICCAIS48893.2020.9096809.

ARMIJO-CORREA, J.O., MURGUÍA, J.S., MEJÍA-CARLOS, M., ARCE-GUEVARA, V.E. AND ABOYTES-GONZÁLEZ, J.A., 2020. An improved visually meaningful encrypted image scheme. Optics and Laser Technology, 127(January), p.106165. https://doi.org/10.1016/j.optlastec.2020.106165.

CHOWDHARY, C.L., PATEL, P.V., KATHROTIA, K.J., ATTIQUE, M., KUMARESAN, P. AND IJAZ, M.F., 2020. Analytical study of hybrid techniques for image encryption and decryption. Sensors (Switzerland), 20(18), pp.1–19. https://doi.org/10.3390/s20185162.

FIGUEROA, D.E., 2023. Compromising sensitive information through Padding Oracle and Known Plaintext attacks in Encrypt-then-TLS scenarios Padding Oracle attack in AES-CBC. pp.1–6.

G, E.J., A, H.M. AND S, F.H.M., 2022. Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography. International Journal of Advanced Computer Science and Applications, 13(8), pp.899–905. https://doi.org/10.14569/ijacsa.2022.0130810 4.

GEETHA, B.T., MOHAN, P., MAYURI, A.V.R., JACKULIN, T., ALDO STALIN, J.L. AND ANITHA, V., 2022. Pigeon Inspired Optimization with Encryption Based Secure Medical Image Management System. Computational Intelligence and Neuroscience, 2022(Cc). https://doi.org/10.1155/2022/2243827.

GUPTA, N. AND VIJAY, R., 2022. Hybrid image compression-encryption scheme based on multilayer stacked autoencoder and logistic map. China Communications, 19(1), pp.238–252. https://doi.org/10.23919/JCC.2022.01.017.

HIDAYATI, L.N., FITRIANA, G.F. AND ADAM, I.F., 2021. Perbandingan Keacakan Citra Enkripsi Algoritma AES dan Camelia Uji NPCR dan UACI. JURIKOM (Jurnal Riset Komputer), 8(6), p.274. https://doi.org/10.30865/jurikom.v8i6.3624.

ISMADIAH, R., SYAHRIZAL, M. AND RAMADHANI, P., 2020. Kombinasi Algoritma Cipher Block Chaining (CBC) dan Mars Pada Penyandian File PDF. Journal of Computer System and Informatics (JoSYC),

1(4), pp.337–345.

MAHMUD, W. AND MINTORINI, E., 2020. Pengamanan Data Kombinasi Metode Cipher Block Chaining dan Modifikasi LSB. Techno.Com, 19(1), pp.97–102. https://doi.org/10.33633/tc.v19i1.3375.

MALIK, A., HE, P., WANG, H., KHAN, A.N., PIRASTEH, S. AND ABDULLAHI, S.M., 2020. High-Capacity Reversible Data Hiding in Encrypted Images Using Multi-Layer Embedding. IEEE Access, 8, pp.148997–149010. https://doi.org/10.1109/ACCESS.2020.3015882.

NOSHADIAN, S., EBRAHIMZADE, A. AND KAZEMITABAR, S.J., 2020. Breaking a chaotic image encryption algorithm. Multimedia Tools and Applications, 79(35–36), pp.25635–25655. https://doi.org/10.1007/s11042-020-09233-6.

NURHANDHI, M. AND SUHENDAR, A., 2023. Improving Firebase BaaS Service Security in Counseling Chat Applications: AES-256 and CBC Approach for End-to-End Encryption. JISA(Jurnal Informatika dan Sains), 6(2), pp.153–160. https://doi.org/10.31326/jisa.v6i2.1783.

PARVATHRAJ, K.M.M. AND ANOOP, B.K., 2023. An Image Encryption Model Using Hyper Chaotic Map Dependent Grey-Intelligent Optimization. Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023, pp.301–306. https://doi.org/10.1109/ICPCSN58827.2023.00056.

REZNIK, Y., 2023. Another Look at SSIM Image Quality Metric. IS and T International Symposium on Electronic Imaging Science and Technology, 35(8), pp.1–7. https://doi.org/10.2352/EI.2023.35.8.IQSP-305.

SANKPAL, P.R. AND VIJAYA, P.A., 2021. Performance Evaluation of Nested Watermarked Scheme using Objective Image Quality Metrics. Journal of University of Shanghai for Science and Technology, 23(06), pp.306–314. https://doi.org/10.51201/jusst/21/05273.

SARA, U., AKTER, M. AND UDDIN, M.S., 2019. Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. Journal of Computer and Communications, 07(03), pp.8–18. https://doi.org/10.4236/jcc.2019.73002.

SETIADI, D.R.I.M., 2020. PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-020-10035-z.

SETIADI, D.R.I.M., RACHMAWANTO, E.H., SARI, C.A., SUSANTO, A. AND DOHEIR, M., 2018. A Comparative Study of Image Cryptographic Method. Proceedings - 2018 5th International Conference on Information Technology, Computer and Electrical Engineering, ICITACEE 2018, pp.336–341. https://doi.org/10.1109/ICITACEE.2018.8576907.

SINGH, A., AGARWAL, P. AND CHAND, M., 2019. Image Encryption and Analysis using Dynamic AES. 2019 International Conference on Optimization and Applications, ICOA 2019, pp.1–6. https://doi.org/10.1109/ICOA.2019.8727711.

WANG, J., CHEN, P., ZHENG, N., CHEN, B., PRINCIPE, J.C. AND WANG, F.Y., 2021. Associations between MSE and SSIM as cost functions in linear decomposition with application to bit allocation for sparse coding. Neurocomputing, 422, pp.139–149. https://doi.org/10.1016/j.neucom.2020.10.018

YAN, X., WANG, X. AND XIAN, Y., 2021. Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. Multimedia Tools and Applications, 80(7), pp.10949–10983. https://doi.org/10.1007/s11042-020-10218-8.

Study ini merupakan bagian dari penelitian yang didukung dari Direktorat Riset, Teknologi dan Pengabdian kepada Masyarakat, KemDikBud dan Ristek dengan no kontrak No.0609.12/LL5-INT/Al.04/2024 and 044/PFR/LPPM-UAD/VI/2024