Analisis Kelemahan AES-ECB Pada Enkripsi Citra dan Mitigasinya dengan CBC/CTR

Axel Santadi Warih , 13522155[1,2]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13522155@std.stei.itb.ac.id, [2]axelsantadi@gmail.com

Abstract*—Advanced Encryption Standard (AES) banyak digunakan untuk menjaga kerahasiaan data, namun tingkat keamanannya sangat dipengaruhi oleh mode operasi yang dipilih. Pada enkripsi citra menggunakan mode Electronic Codebook (ECB), blok plaintext yang identik akan menghasilkan blok ciphertext yang identik, sehingga pola dan struktur visual citra masih dapat "bocor" dan dikenali. Makalah ini menganalisis kelemahan praktis AES-ECB pada enkripsi citra serta mengevaluasi mode Cipher Block Chaining (CBC) dan Counter (CTR) sebagai mitigasi. Saya mengimplementasikan enkripsi citra berbasis AES pada mode ECB, CBC, dan CTR, kemudian melakukan eksperimen pada beberapa citra grayscale dan RGB. Evaluasi dilakukan melalui (i) inspeksi visual pada citra hasil enkripsi untuk melihat sisa pola, (ii) karakteristik histogram ciphertext dan entropi Shannon, (iii) korelasi piksel bertetangga, serta (iv) waktu eksekusi. Hasil eksperimen menunjukkan bahwa mode ECB masih mempertahankan kontur/tekstur tertentu sehingga informasi visual dapat tertebak, sedangkan CBC dan CTR efektif menghilangkan pola yang bermakna dan menghasilkan statistik ciphertext yang lebih mendekati acak. CTR menunjukkan kinerja yang relatif mendekati ECB, sementara CBC menambah overhead akibat ketergantungan chaining. Temuan ini menegaskan bahwa ECB tidak tepat digunakan untuk enkripsi citra, dan CBC/CTR dengan IV/nonce acak yang selalu baru merupakan pilihan mitigasi yang praktis.

***Keywords*—AES, enkripsi citra, ECB, CBC, CTR, kebocoran pola**

I. PENDAHULUAN

Pertukaran citra digital melalui jaringan publik (misalnya internet) semakin masif, baik untuk kebutuhan personal maupun institusional, sehingga kerahasiaan dan privasi data citra menjadi isu keamanan yang penting. Pada praktiknya, citra memiliki redundansi yang tinggi karena adanya korelasi antar-piksel yang bertetangga, sehingga pola dan struktur visual sering kali "terulang" di banyak bagian gambar. Karena karakteristik tersebut, penerapan kriptografi pada citra perlu dievaluasi secara hati-hati, terutama terkait apakah hasil enkripsi benar-benar menyembunyikan pola visual yang bermakna.

Salah satu algoritma kriptografi yang paling umum digunakan untuk perlindungan kerahasiaan data adalah Advanced Encryption Standard (AES). AES merupakan block cipher simetris yang distandarisasi oleh NIST, mendukung ukuran kunci 128/192/256-bit dan memproses data dalam blok 128-bit. Namun, block cipher seperti AES tidak berdiri sendiri untuk data berukuran panjang; ia membutuhkan mode operasi untuk memproses rangkaian blok secara berulang, misalnya ECB, CBC, dan CTR. Pilihan mode operasi sangat menentukan sifat keamanan dan "jejak" pola yang mungkin masih tampak pada ciphertext, khususnya untuk data yang kaya struktur seperti citra.

Mode Electronic Codebook (ECB) mengenkripsi setiap blok plaintext secara independen. Dalam rekomendasi NIST untuk mode operasi block cipher, ditegaskan bahwa pada ECB, "di bawah satu kunci yang sama, blok plaintext yang sama akan selalu terenkripsi menjadi blok ciphertext yang sama"; apabila sifat ini tidak diinginkan, maka ECB sebaiknya tidak digunakan. Pada konteks citra, sifat deterministik ini menjadi masalah: area gambar yang serupa atau berulang (misalnya latar belakang polos, pola tekstur, atau kontur objek) cenderung membentuk blok-blok plaintext yang identik, sehingga menghasilkan blok ciphertext yang identik pula. Akibatnya, meskipun nilai piksel sudah terenkripsi, struktur visual (kontur/tekstur) dapat masih "terbaca" secara kasat mata dari hasil enkripsi.

Untuk memitigasi kelemahan tersebut, makalah ini membahas dua mode operasi yang umum dipakai, yaitu Cipher Block Chaining (CBC) dan Counter (CTR). CBC menggabungkan (chaining) blok plaintext dengan blok ciphertext sebelumnya, dan membutuhkan Initialization Vector (IV) untuk blok pertama; NIST menekankan IV tidak perlu rahasia, tetapi harus tidak dapat diprediksi (unpredictable), serta integritas IV perlu diproteksi. Sementara itu, CTR menghasilkan keystream dari enkripsi "counter block" dan meng-XOR-kan ke plaintext; NIST mensyaratkan counter block yang unik untuk setiap blok plaintext yang pernah dienkripsi di bawah kunci yang sama (lintas semua pesan), karena reuse counter dapat mengompromikan kerahasiaan plaintext. Dengan demikian, CBC/CTR secara desain ditujukan untuk menghindari pemetaan deterministik "blok sama → ciphertext sama" yang menjadi akar kebocoran pola pada ECB.

Berdasarkan latar belakang tersebut, tujuan makalah ini adalah: (1) menunjukkan kelemahan AES-ECB pada enkripsi citra secara praktis, (2) mengevaluasi CBC dan CTR sebagai mitigasi kebocoran pola, serta (3) membandingkan karakteristik hasil enkripsi dan dampak kinerjanya secara eksperimen. Saya mengimplementasikan enkripsi–dekripsi citra menggunakan AES pada mode ECB, CBC, dan CTR, kemudian melakukan pengujian pada beberapa citra grayscale dan RGB. Evaluasi dilakukan melalui inspeksi visual ciphertext (apakah pola masih tampak) dan indikator statistik yang lazim digunakan dalam evaluasi enkripsi citra, seperti histogram, entropi, dan korelasi piksel bertetangga. Saya juga melakukan pengukuran waktu eksekusi untuk melihat trade-off performa antar mode.

II. Landasan Teori

Algoritma Advanced Encryption Standard (AES) merupakan block cipher kunci-simetri yang distandardisasi oleh NIST. Standar ini mendefinisikan tiga varian, yaitu AES-128, AES-192, dan AES-256, di mana sufiks menunjukkan panjang kunci, sementara ukuran blok (input/output) selalu 128-bit. Jumlah putaran (round) yang digunakan adalah 10, 12, dan 14 untuk AES-128, AES-192, dan AES-256. Selain itu, AES bekerja pada *state* berukuran 4×4 byte (16 byte = 128 bit) dan mengaplikasikan transformasi utama seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey, dengan *key schedule* untuk membangkitkan round key pada tiap putaran.

Karena AES adalah block cipher, data yang lebih panjang dari satu blok harus diproses dengan mode operasi (mode of operation). NIST mendefinisikan beberapa mode standar untuk block cipher, termasuk ECB (Electronic Codebook), CBC (Cipher Block Chaining), dan CTR (Counter), yang masing-masing menentukan cara memetakan blok-blok plaintext menjadi blok-blok ciphertext agar dapat menangani pesan multi-blok.

Mode ECB mendefinisikan enkripsi per blok secara independen:

$$C_j = E_K(P_j)$$

dan dekripsi:

$$P_j = D_K(C_j)$$

sehingga blok plaintext yang sama akan selalu menghasilkan blok ciphertext yang sama di bawah kunci yang sama. NIST menyatakan (kutipan singkat): *"any given plaintext block always gets encrypted to the same ciphertext block"* sehingga bila sifat ini tidak diinginkan, ECB tidak seharusnya digunakan. Dalam konteks citra, ini krusial karena citra umumnya memiliki pola/redundansi (misalnya area warna seragam) yang dapat menghasilkan blok-blok plaintext identik, lalu tercermin sebagai pola visual pada ciphertext-image.

Mode **CBC** memperkenalkan keterkaitan antar blok melalui operasi XOR dengan ciphertext blok sebelumnya, dengan definisi:

$$C_1 = E_K(P_1 \oplus IV), C_j = E_K(P_j \oplus C_{j-1}),$$

dan dekripsi:

$$P_1 = D_K(C_1) \oplus IV, P_j = D_K(C_j) \oplus C_{j-1},$$

Dengan chaining ini, dua blok plaintext yang sama (pada posisi berbeda) tidak otomatis menghasilkan ciphertext yang sama karena bergantung pada C_{j-1}. Keamanan CBC juga sangat dipengaruhi oleh IV: untuk mode chaining tertentu, NIST menekankan IV harus tak terprediksi (unpredictable).

Mode CTR mengubah AES menjadi skema mirip stream cipher, dengan cara mengenkripsi *counter block* lalu melakukan XOR ke plaintext:

$$C_j = P_j \oplus E_K(T_j)$$

di mana T_j dibangun dari nonce/counter. Keamanan CTR sangat bergantung pada aturan keunikan counter block: NIST menegaskan *counter blocks are distinct across all messages that are ever encrypted under a given key*. Artinya, reuse nonce/counter pada kunci yang sama berisiko fatal (menghasilkan *keystream reuse*).

Dalam praktik implementasi pada data berukuran arbitrer (termasuk citra), persoalan penting adalah padding. NIST membahas *padding* untuk menyesuaikan panjang plaintext ke kelipatan ukuran blok (128-bit untuk AES), khususnya relevan untuk mode seperti ECB dan CBC yang memproses blok utuh. Sementara itu, CTR sering lebih fleksibel karena bekerja dengan XOR *keystream*, namun tetap harus memperlakukan bagian akhir pesan secara konsisten dan aman.

Perlu dicatat bahwa ECB/CBC/CTR pada dasarnya berfokus pada kerahasiaan (confidentiality). Dalam sistem riil, enkripsi tanpa autentikasi masih rentan manipulasi (mis. bit-flipping pada mode tertentu). Karena itu, praktik yang umum direkomendasikan adalah memakai skema authenticated encryption (contoh: GCM) untuk sekaligus menjamin confidentiality dan integrity/authentication. (Bagian ini menjadi konteks, walau eksperimen makalah berfokus pada kebocoran pola ECB dan mitigasinya dengan CBC/CTR.)

Citra digital dapat dipandang sebagai berkas data yang menyimpan array 2D/kanal piksel, dan pada umumnya memiliki redundansi tinggi akibat korelasi antar piksel bertetangga. Literatur survei evaluasi enkripsi citra menekankan bahwa korelasi tetangga ini adalah alasan mengapa evaluasi enkripsi citra sering mengukur "seberapa acak" ciphertext-image melalui metrik seperti histogram analysis, entropy, dan correlation coefficient.

Untuk menilai kualitas enkripsi citra dalam eksperimen, beberapa metrik yang lazim digunakan adalah: (1) analisis histogram, (2) entropi informasi, dan (3) korelasi piksel bertetangga. Histogram ciphertext-image yang "mendekati seragam" biasanya diinterpretasikan sebagai indikasi bahwa distribusi intensitas piksel tidak lagi memuat pola yang mudah dieksploitasi. Survei metrik evaluasi enkripsi citra merangkum histogram sebagai salah satu indikator kualitas keamanan/acaknya cipher-image.

Entropi informasi (Shannon entropy) sering dipakai untuk mengukur tingkat ketidakpastian/keacakan distribusi simbol (mis. nilai piksel 0–255). Secara umum didefinisikan sebagai:

$$H(X) = -\sum_{x} p(x)\, log_2\, p(x)$$

Konsep entropi ini berasal dari teori informasi Shannon dan kerap dijadikan dasar untuk mengukur "randomness" pada data hasil enkripsi. Dalam evaluasi citra, nilai entropi ciphertext-image yang lebih tinggi (mendekati maksimum teoretis untuk 8-bit) biasanya mengindikasikan distribusi nilai piksel yang lebih mendekati acak.

Korelasi piksel bertetangga mengukur seberapa kuat hubungan linear antara pasangan piksel (mis. horizontal/vertikal/diagonal). Pada citra plaintext alami, korelasi ini umumnya tinggi, sedangkan pada ciphertext-image yang baik, korelasi diharapkan turun mendekati nol. Pengukuran korelasi dan distribusinya sering digunakan sebagai metrik evaluasi pada studi enkripsi citra.

III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode eksperimen implementatif untuk menganalisis kebocoran pola pada enkripsi citra menggunakan AES-ECB serta mengevaluasi CBC dan CTR sebagai mitigasi. Implementasi dilakukan dengan menerapkan AES sebagai block cipher berukuran blok 128-bit pada data citra yang direpresentasikan sebagai deretan byte piksel, lalu membandingkan keluaran ciphertext-image dari tiga mode operasi. AES dipilih karena merupakan standar enkripsi simetris yang banyak digunakan dan didefinisikan oleh NIST. Mode operasi yang diuji (ECB, CBC, CTR) mengacu pada rekomendasi NIST untuk mode operasi block cipher.

Dataset citra yang digunakan diambil dari USC-SIPI Image Database, karena merupakan koleksi citra standar yang sering dipakai untuk riset pengolahan citra. Untuk memudahkan rekonstruksi ciphertext menjadi citra (agar bisa dinilai secara visual), saya memilih citra dengan ukuran resolusi yang "ramah blok", misalnya 512×512, sehingga jumlah byte piksel (baik grayscale maupun RGB) merupakan kelipatan 16 dan tidak memerlukan penanganan padding yang rumit pada ECB/CBC. (Apabila pada variasi uji tertentu ukuran citra tidak kelipatan 16, maka padding diterapkan menggunakan skema PKCS#7 sebagaimana dijelaskan dalam RFC 5652).

Selain citra dari USC-SIPI Image Database, saya juga menggunakan satu citra terstruktur berupa logo (logo ITB) sebagai kasus uji tambahan. Citra terstruktur memiliki area warna seragam dan pola berulang yang lebih jelas, sehingga memudahkan observasi kebocoran pola pada mode ECB dibanding citra natural. Seluruh citra diproses dalam format 8-bit per kanal (RGB atau grayscale) dan diserialisasi menjadi byte array sebelum dienkripsi.

Tahap pra-pemrosesan dilakukan dengan memuat citra, mengubahnya ke representasi 8-bit per kanal (grayscale: 1 kanal; RGB: 3 kanal), lalu mengekstraksi matriks piksel menjadi *byte array* berurutan. Byte array inilah yang dianggap sebagai plaintext. Setelah proses enkripsi, ciphertext (yang juga berupa byte array) dibentuk kembali ke dimensi semula untuk menghasilkan ciphertext-image sehingga perbandingan pola dapat dilakukan secara langsung (misalnya apakah kontur objek masih tampak pada hasil enkripsi).

Eksperimen menggunakan satu kunci AES (misalnya AES-128) untuk menjaga konsistensi pembandingan antar mode pada satu sesi uji. AES memiliki ukuran blok 128-bit dan jumlah ronde bergantung pada panjang kunci, sebagaimana dijelaskan pada standar NIST. Pada mode ECB, setiap blok 16-byte dienkripsi secara independen sehingga plaintext blok yang identik akan menghasilkan ciphertext blok yang identik di bawah kunci yang sama; sifat deterministik inilah yang diuji dampaknya pada citra. Pada mode CBC, setiap blok plaintext di-*XOR* dengan ciphertext blok sebelumnya, dan blok pertama menggunakan Initialization Vector (IV). Sesuai rekomendasi NIST, IV pada CBC harus tidak dapat diprediksi (unpredictable); IV tidak wajib dirahasiakan, tetapi harus dihasilkan secara aman dan disertakan agar dekripsi dapat dilakukan. Pada mode CTR, enkripsi dilakukan dengan membangkitkan *keystream* dari enkripsi *counter block* dan meng-*XOR*-kannya dengan plaintext. CTR mensyaratkan *counter block* yang unik untuk setiap blok plaintext yang pernah dienkripsi di bawah kunci yang sama (lintas semua pesan), sehingga percobaan ini menghasilkan nonce/counter yang tidak pernah diulang.

Implementasi dilakukan menggunakan Python dengan pustaka kriptografi (AES) dan pemrosesan citra. Untuk ECB dan CBC, plaintext dipadding menggunakan PKCS#7 agar panjang data menjadi kelipatan 16 byte; untuk kebutuhan visualisasi ciphertext-image, ciphertext dipotong sepanjang plaintext agar dimensi citra tetap sama. Untuk CTR, ciphertext memiliki panjang yang sama dengan plaintext sehingga tidak memerlukan padding. Pengukuran waktu enkripsi dilakukan dengan menjalankan proses enkripsi berulang sebanyak *5* kali per citra dan melaporkan rata-rata serta simpangan baku. Korelasi piksel bertetangga dihitung dari sampel pasangan piksel acak sebanyak *20.000* pasangan untuk tiap arah (horizontal/vertikal/diagonal) agar hasil stabil.

Evaluasi hasil enkripsi dilakukan melalui dua jalur: evaluasi visual dan evaluasi statistik sederhana yang umum dipakai pada studi enkripsi citra. Literatur survei metrik enkripsi citra merangkum penggunaan analisis histogram, entropi, dan korelasi piksel bertetangga sebagai indikator apakah ciphertext-image "mendekati acak" dan tidak lagi mempertahankan struktur plaintext. Secara visual, saya membandingkan ciphertext-image dari ECB, CBC, dan CTR untuk melihat apakah pola/outline masih dapat dikenali. Secara statistik, saya menghitung histogram intensitas piksel per kanal, serta menghitung entropi Shannon pada distribusi nilai piksel untuk melihat kecenderungan menuju distribusi acak. Konsep entropi informasi mengacu pada teori informasi Shannon. Selain itu, saya mengukur korelasi piksel bertetangga (horizontal, vertikal, diagonal) menggunakan koefisien korelasi Pearson pada pasangan piksel yang diambil dari ciphertext-image; target yang diharapkan adalah korelasi mendekati nol pada hasil enkripsi yang baik. Untuk penentuan jumlah sampel pasangan piksel, praktik umum di literatur enkripsi

citra adalah mengambil ribuan hingga puluhan ribu pasangan piksel secara acak agar hasil korelasi stabil.

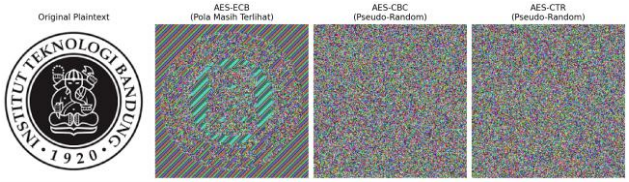
Selain kualitas "pengaburan pola", aspek performa diukur menggunakan waktu eksekusi enkripsi dan dekripsi pada tiap mode. Pengukuran dilakukan dengan menjalankan enkripsi (dan dekripsi) beberapa kali per citra dan melaporkan nilai rata-rata agar variasi *runtime noise* berkurang. Mode CTR secara teori mendukung pemrosesan paralel per blok dan sering kali kompetitif secara performa, sedangkan CBC memiliki ketergantungan antarblok karena chaining sehingga dapat menambah overhead. Penjelasan karakteristik dasar mode-mode ini merujuk pada definisi mode operasi yang disediakan dalam rekomendasi NIST.

Terakhir, untuk menjaga validitas kesimpulan, saya membedakan secara eksplisit antara "mode yang menghilangkan pola visual" dan "keamanan sistem secara menyeluruh". Mode ECB/CBC/CTR yang dibahas pada makalah ini terutama memberikan confidentiality, sementara kebutuhan integritas/autentikasi (misalnya menggunakan skema authenticated encryption) berada di luar fokus eksperimen dan hanya dicatat sebagai batasan penelitian.

IV. Hasil dan Pembahasan

Pada bab ini saya membahas hasil eksperimen enkripsi citra menggunakan AES-128 pada tiga mode operasi: ECB, CBC, dan CTR. AES sendiri merupakan block cipher simetris yang distandarkan oleh NIST dan bekerja pada blok 128-bit. Evaluasi dilakukan dengan dua pendekatan: (1) inspeksi visual citra hasil enkripsi, dan (2) metrik kuantitatif yang umum dipakai pada evaluasi enkripsi citra, yaitu *Shannon entropy* (untuk mengukur "kerandoman" distribusi intensitas) serta korelasi piksel bertetangga (horizontal, vertikal, diagonal) untuk menilai apakah struktur lokal masih "terbaca" setelah dienkripsi. Metrik-metrik ini sering digunakan dalam literatur survei evaluasi enkripsi citra.

Secara visual, hasil eksperimen menunjukkan perbedaan yang paling jelas pada mode ECB. Pada ECB, setiap blok plaintext diproses secara independen, sehingga blok plaintext yang identik akan menghasilkan blok ciphertext yang identik untuk kunci yang sama. Konsekuensinya, pola berulang pada citra (misalnya area warna datar/tepi yang berulang) masih "bocor" dan dapat terlihat sebagai struktur kasar pada citra terenkripsi. Sebaliknya, CBC melakukan *chaining* antarblok (melalui XOR dengan ciphertext blok sebelumnya) dan membutuhkan IV pada blok pertama, sedangkan CTR menggunakan *keystream* berbasis counter sehingga tiap blok efektif "dirandomisasi" oleh urutan counter yang unik; kedua mode ini menghilangkan pola visual dan menghasilkan tampilan *pseudo-random* pada citra ciphertext.



Gambar I. Perbandingan hasil enkripsi citra logo (terstruktur) menggunakan AES-128 pada mode ECB, CBC, dan CTR.

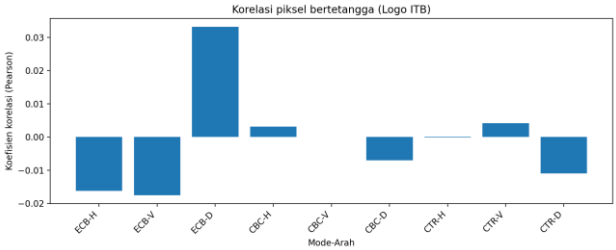
Pada citra yang relatif terstruktur (logo), mode ECB menunjukkan penurunan entropy yang signifikan dibanding CBC/CTR. Hal ini konsisten dengan kebocoran pola: ciphertext ECB cenderung memiliki distribusi intensitas yang tidak se-"acak" CBC/CTR karena masih memuat regularitas blok. Korelasi diagonal pada ECB juga lebih tinggi dibanding CBC/CTR, yang mengindikasikan masih ada keteraturan spasial yang tidak sepenuhnya hilang.

Mode	Entropy rata-rata	Corr(H)	Corr(V)	Corr(D)	Waktu enkripsi rata-rata (s)
ECB	6.8483	-0.0162	-0.0175	0.0332	0.000940
CBC	7.9962	0.0031	0.0000	-0.0070	0.001005
CTR	7.9962	-0.0002	0.0042	-0.0109	0.001049

Tabel I. Hasil Uji Gambar Logo ITB

Dari Tabel I terlihat bahwa CBC dan CTR menghasilkan entropy mendekati nilai maksimum 8 bit per kanal (untuk 8-bit intensitas), sedangkan ECB jauh lebih rendah. Secara interpretasi, CBC/CTR telah "menghapus" jejak struktur histogram dan hubungan spasial, sementara ECB masih menyisakan keteraturan yang bisa diamati, terutama pada citra dengan pola jelas.

Eksperimen juga dijalankan pada beberapa citra natural dari USC-SIPI Image Database, yang memang sering digunakan untuk riset pemrosesan citra. Pada kelompok citra ini, hasil entropy untuk ketiga mode sangat tinggi dan saling berdekatan (≈7.999–8.000), dan korelasi piksel bertetangga juga berada di sekitar nol untuk semua mode. Ini berarti, untuk citra natural yang kompleks, metrik global seperti entropy rata-rata cenderung "jenuh" dan menjadi kurang sensitif membedakan kebocoran pola halus pada ECB.



Gambar II. Hasil Korelasi Piksel

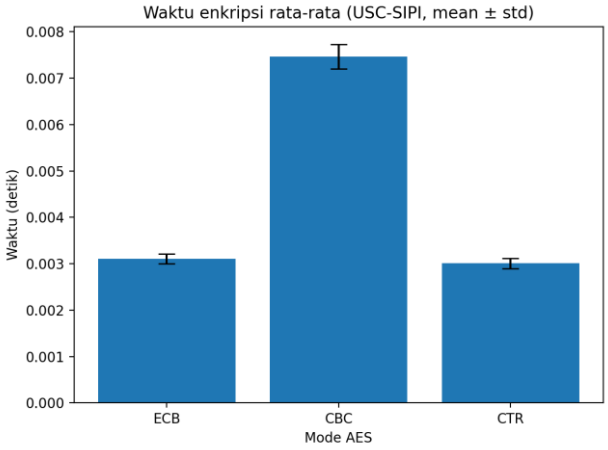
Mode	Entropy rata-rata (mean ± std)	Corr(H) mean	Corr(V) mean	Corr(D) mean	Waktu enkripsi (s) mean ± std
ECB	7.999786 ± 0.000064	0.002537	0.001114	-0.002176	0.003110 ± 0.000107
CBC	7.999822 ± 0.000008	-0.001603	-0.004578	0.006254	0.007462 ± 0.000265
CTR	7.999824 ± 0.000004	0.002156	-0.000194	-0.004603	0.003008 ± 0.000114

Tabel II. Hasil Uji Gambar SIPI

Fenomena "nilai entropy sama-sama tinggi" pada citra natural ini sejalan dengan kritik di literatur bahwa *global Shannon entropy* memiliki keterbatasan untuk membedakan tingkat kerandoman citra dalam beberapa kasus (misalnya sebelum/sesudah *shuffling* atau untuk perbandingan yang lebih adil lintas ukuran/konten), sehingga diusulkan ukuran berbasis *local entropy* sebagai alternatif yang lebih peka. Dengan demikian, inspeksi visual tetap menjadi indikator paling kuat untuk menunjukkan kelemahan ECB pada citra yang memiliki struktur/pola jelas, sedangkan untuk citra natural perlu metrik tambahan agar perbedaan antar-mode lebih "terbaca" secara kuantitatif (mis. *local entropy*, uji keacakan blok, NPCR/UACI, dan sebagainya).

Sebagai metrik tambahan untuk menangkap karakter deterministik ECB, saya menghitung tingkat repetisi blok ciphertext berukuran 16 byte. Repetition rate didefinisikan sebagai $Repetition\ Rate = 1 - \frac{|unique\ blocks|}{|total\ blocks|}$. Pada ECB, citra dengan area/pola berulang cenderung menghasilkan repetition rate lebih tinggi karena blok plaintext identik akan memetakan ke blok ciphertext identik. Sebaliknya, pada CBC/CTR, penggunaan IV/nonce/counter menyebabkan blok ciphertext cenderung berbeda sehingga repetition rate turun.

Dari sisi waktu eksekusi, CTR dan ECB cenderung lebih cepat daripada CBC pada citra SIPI yang lebih besar (Tabel II). Secara konseptual ini masuk akal karena CBC memiliki dependensi antarblok saat enkripsi (chaining), sedangkan CTR menghasilkan *keystream* berbasis counter dan lebih mudah diparalelkan. Namun, aspek performa tidak boleh mengorbankan keamanan implementasi: CBC mensyaratkan IV yang tidak dapat diprediksi (unpredictable) dan integritas IV perlu diperhatikan, sedangkan CTR mensyaratkan counter block yang unik (tidak pernah terulang untuk kunci yang sama) agar tidak terjadi reuse keystream. Dalam konteks enkripsi citra, hasil eksperimen menegaskan bahwa ECB tidak cocok digunakan karena kebocoran pola, sedangkan CBC/CTR efektif sebagai mitigasi asalkan IV/counter dikelola sesuai ketentuan standar.



Gambar III. Rata - rata waktu eksekusi ECB, CBC dan CTR.

V. KESIMPULAN

Berdasarkan implementasi dan eksperimen enkripsi citra menggunakan AES-128 pada mode ECB, CBC, dan CTR, dapat disimpulkan bahwa mode operasi sangat memengaruhi kebocoran informasi pada ciphertext-image. Mode ECB menunjukkan kelemahan utama berupa kebocoran pola karena setiap blok plaintext dienkripsi secara independen; blok plaintext yang identik menghasilkan blok ciphertext yang identik, sehingga struktur citra terstruktur (misalnya logo) masih dapat terlihat pada hasil enkripsi. Sebaliknya, mode CBC dan CTR mampu memitigasi kebocoran pola tersebut dan menghasilkan ciphertext-image yang tampak pseudo-random, ditunjukkan pula oleh metrik entropi yang mendekati maksimum serta korelasi piksel bertetangga yang mendekati nol pada hasil enkripsi.

Dari sisi performa, CTR cenderung memberikan waktu enkripsi yang kompetitif dibanding CBC pada citra berukuran besar, sedangkan CBC dapat menambah overhead akibat mekanisme chaining antarblok. Namun, efektivitas CBC/CTR tetap bergantung pada pengelolaan parameter dengan benar, yaitu penggunaan IV yang tidak dapat diprediksi pada CBC serta nonce/counter yang unik pada CTR agar tidak terjadi reuse yang membahayakan kerahasiaan.

REFERENCES

[1] National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), 2001. [Online]. Available: https://csrc.nist.gov/pubs/fips/197/final. Accessed: 17-Dec-2025 13:44 WIB.

[2] M. Dworkin (NIST), SP 800-38A: Recommendation for Block Cipher Modes of Operation—Methods and Techniques, 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf. Accessed: 17-Dec-2025 14:13 WIB.

[3] Y. Wu, J. P. Noonan, and S. Agaian, "Local Shannon entropy measure with statistical tests for image randomness," Information Sciences, 2013. [Online]. Available: https://doi.org/10.1016/j.ins.2012.07.049. Accessed: 17-Dec-2025 15:33 WIB.

[4] A. G. Weber, The USC-SIPI Image Database: Version 6, USC-SIPI Report #432, 2018. [Online]. Available:

https://sipi.usc.edu/database/SIPI_Database.pdf. Accessed: 17-Dec-2025 20:11 WIB.
[5] R. Housley, “Cryptographic Message Syntax (CMS),” RFC 5652, 2009. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5652.html. Accessed: 17-Dec-2025 21:57 WIB.
[6] M. Dworkin (NIST), SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38d.pdf. Accessed: 18-Dec-2025 01:22 WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Desember 2025

Axel Santadi Warih 13522155