Paper

Enkripsi Citra Digital dengan IDEA Cipher: Pengacakan Blok Pseudorandom LCG dan Evaluasi Melalui Image Correlation Analysis

Author : Manovri Yeni, Tommy, Rosyidah Siregar

SNASTIKOM 10
Seminar Nasional Teknologi Informasi dan Komunikasi
UNIVERSITAS HARAPAN MEDAN 2012-2023
Program Studi Teknik Informatika
TEMA : DUNIA AKADEMIK DI ERA SOCIETY 5.0 : TANTANGAN DAN PELUANG
ISSN : 2964-1950

ISSN: 2964-1950

Enkripsi Citra Digital dengan IDEA Cipher: Pengacakan Blok Pseudorandom LCG dan Evaluasi Melalui Image Correlation Analysis

Manovri Yeni[1], Tommy[2*], Rosyidah Siregar[3]
[1] Universitas Muhammadiyah Aceh, Banda Aceh, Indonesia
[2*,3]Universitas Harapan Medan, Medan, Indonesia
[1]manovri.yeni@unmuha.ac.id, [2*]tomshirakawa@gmail.com, [3*]rosyidah_siregar.unhar@harapan.ac.id
[*)]Email Penulis Korespondensi

Abstrak

Penggunaan metode kriptografi pada pengolahan citra digital telah menjadi fokus penelitian yang penting dalam menjaga keamanan informasi visual. Penelitian ini menganalisis penggunaan Linear Congruential Generator (LCG) sebagai alat pengacakan blok pada proses enkripsi citra menggunakan algoritma International Data Encryption Algorithm (IDEA). Tujuan penelitian ini adalah untuk mengevaluasi efektivitas LCG dalam mengurangi pola korelasi antar blok piksel dalam citra terenkripsi. Dalam eksperimen yang dilakukan menggunakan dataset citra dari OpenDataset, hasil pengujian menunjukkan perbedaan yang signifikan antara enkripsi citra menggunakan IDEA biasa dan IDEA yang didukung dengan LCG. Metode pengacakan blok dengan LCG berhasil menghasilkan citra terenkripsi dengan nilai korelasi koefisien yang mendekati nol, menandakan efektivitasnya dalam mengaburkan pola korelasi antar blok piksel. Meskipun terdapat penurunan Mean Squared Error (MSE) dan sedikit degradasi kualitas citra terenkripsi, hasil evaluasi menegaskan peningkatan signifikan pada perbaikan koefisien korelasi rata-rata sebesar 4.57. Hal ini mengindikasikan peningkatan keamanan citra terenkripsi terhadap serangan kriptanalisis yang memanfaatkan pola korelasi, dengan mempertimbangkan kompromi pada kualitas citra. Hasil penelitian ini menegaskan bahwa penggunaan LCG dalam pengacakan blok pada enkripsi citra dengan IDEA mampu menghasilkan citra terenkripsi dengan tingkat keamanan yang lebih tinggi melalui pengurangan pola korelasi, meskipun dengan sedikit pengorbanan pada kualitas citra. Implikasi dari temuan ini dapat memberikan kontribusi pada pengembangan metode keamanan pada pengolahan citra digital di masa mendatang.

Kata Kunci: Kriptografi, Citra Digital, LCG, IDEA, Koefisien Korelasi

Abstract

The use of cryptography methods in digital image processing has become a crucial focus of research in safeguarding visual information. This study analyzes the utilization of the Linear Congruential Generator (LCG) as a block scrambling tool in the image encryption process using the International Data Encryption Algorithm (IDEA). The aim of this research is to evaluate the effectiveness of LCG in reducing correlation patterns among pixel blocks in encrypted images. In experiments conducted using image datasets from OpenDataset, the test results indicated a significant difference between encrypting images using regular IDEA and IDEA enhanced with LCG. The block scrambling method using LCG successfully generated encrypted images with correlation coefficient values approaching zero, signifying its effectiveness in obscuring correlation patterns among pixel blocks. Despite a decrease in Mean Squared Error (MSE) and slight degradation in the quality of the encrypted images, the evaluation results affirmed a significant improvement in the average correlation coefficient by 4.57. This indicates an enhanced security level for encrypted images against cryptanalysis leveraging correlation patterns, while considering compromises in image quality. The findings of this research affirm that utilizing LCG in block scrambling during image encryption with IDEA can produce encrypted images with higher security levels by reducing correlation patterns, albeit with a slight sacrifice in image quality. The implications of these findings might contribute to the development of security methods in digital image processing in the future.

Keywords: *Cryptography, Digital Image, LCG, IDEA, Correlation Coefficient*

1. PENDAHULUAN

Di bidang ilmu citra digital, kriptografi telah mengalami evolusi yang cukup besar dalam upayanya melindungi informasi visual. Penggunaan kriptografi dalam lingkup citra digital tidak hanya berkaitan dengan menjaga kerahasiaan informasi, melainkan juga memastikan integritas dan autentikasi citra selama proses penyimpanan dan pengiriman. Perkembangan ini telah mendorong pengembangan beragam algoritma dan teknik enkripsi yang didesain khusus untuk melindungi citra digital dari akses yang tidak sah. Algoritma kriptografi yang dioptimalkan untuk citra digital memfasilitasi transmisi dan penyimpanan informasi visual yang sensitif dengan tingkat

keamanan yang dibutuhkan di lingkungan digital yang rawan terhadap potensi serangan. Dalam kurun waktu beberapa tahun terakhir, terjadi kemajuan signifikan dalam kriptografi citra digital yang memberikan solusi-solusi yang lebih kompleks dan efisien. Teknik-teknik seperti enkripsi kunci spesifik [1], transformasi permutasi [2], serta teknik steganografi telah mengalami kemajuan yang cukup pesat untuk memastikan keamanan citra digital. Pemanfaatan algoritma kriptografi baik simetris maupun asimetris telah memperkuat perlindungan citra digital, baik dalam hal pengiriman melalui jaringan maupun saat disimpan di berbagai media penyimpanan. Kemajuan ini telah membuka peluang lebih luas bagi penggunaan citra digital di berbagai sektor, dari aplikasi medis [3] hingga keamanan data pribadi dalam penggunaan sehari-hari [4].

Dalam konteks enkripsi blok simetris pada citra digital, permasalahan yang muncul adalah terkait dengan korelasi yang bisa hadir antara blok-blok tertentu dalam hasil enkripsi [5]. Korelasi yang tinggi antar-blok setelah proses enkripsi bisa menjadi celah yang dimanfaatkan oleh pihak yang tidak berwenang untuk mengakses informasi secara tidak sah [6]. Ketika citra dienkripsi menggunakan algoritma blok simetris, blok-blok piksel yang berdekatan dapat menunjukkan korelasi yang tidak diinginkan, sehingga memungkinkan pembacaan atau serangan terhadap citra yang dienkripsi. Bahkan dengan enkripsi yang kuat, korelasi yang masih terlihat pada level blok dapat membuka jendela bagi serangan kriptanalisis yang bertujuan untuk mendekripsi citra. Penting untuk memahami bahwa korelasi ini bukan hanya masalah teoretis, tetapi juga memiliki implikasi praktis yang signifikan. Tingkat korelasi yang terdeteksi pada blok-blok piksel dalam citra hasil enkripsi bisa menjadi indikator penting bagi para penyerang yang berusaha memecahkan kunci enkripsi atau mengungkap informasi yang disembunyikan dalam citra. Oleh karena itu, pengurangan korelasi antar-blok dalam hasil enkripsi menjadi fokus dalam upaya meningkatkan keamanan citra digital dan menjaga kerahasiaan data visual yang sensitif. Upaya-upaya baru terus dilakukan untuk mengatasi masalah korelasi ini dalam enkripsi blok simetris pada citra digital dengan berbagai teknik dan strategi yang bertujuan untuk memperkuat keamanan enkripsi [7] [8].

Penerapan pseudorandom dalam konteks enkripsi citra digital telah menjadi bidang penelitian yang menarik dalam upaya mengatasi masalah korelasi yang timbul pada hasil enkripsi [9]. Pseudorandom, sebagai metode pembangkitan urutan angka yang bersifat hampir acak, digunakan dalam proses enkripsi untuk mengacaukan pola yang mungkin timbul pada blok-blok piksel dalam citra hasil enkripsi. Hal ini bertujuan untuk mengurangi atau menghilangkan korelasi yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Penelitian sebelumnya telah menunjukkan bahwa penerapan pseudorandom dalam enkripsi citra digital mampu meningkatkan tingkat keamanan dengan mengaburkan pola-pola yang muncul dalam citra hasil enkripsi [10]. Dengan menggunakan metode ini, pola korelasi yang biasanya terlihat pada blok-blok piksel dapat diacak sehingga sulit bagi pihak yang tidak memiliki kunci enkripsi untuk menguraikan atau membaca kembali citra asli dari citra hasil enkripsi. Penggunaan pseudorandom sebagai salah satu strategi dalam proses enkripsi citra digital menawarkan kemungkinan untuk meningkatkan tingkat keamanan dalam melindungi data visual.

Linear Congruential Generator (LCG) telah menjadi salah satu metode yang menarik untuk menghasilkan urutan angka pseudorandom dalam proses pengacakan blok dalam enkripsi citra digital [11]. Dalam konteks ini, LCG digunakan untuk menghasilkan deret angka yang hampir acak, yang nantinya akan memengaruhi urutan blok dalam proses enkripsi citra. Penggunaan LCG dalam pengacakan blok bertujuan untuk memperkenalkan tingkat keacakan yang cukup dalam urutan blok enkripsi, sehingga mengurangi atau bahkan menghilangkan pola korelasi yang dapat dimanfaatkan untuk menganalisis citra hasil enkripsi. Penelitian-penelitian sebelumnya telah mengungkap potensi LCG sebagai alternatif yang menarik dalam meningkatkan keamanan enkripsi citra digital [12]. Dengan memanfaatkan kemampuan LCG untuk menghasilkan urutan angka yang bersifat hampir acak, pengacakan blok dalam proses enkripsi dapat menjadi lebih efektif dalam mengaburkan pola yang mungkin muncul pada blok-blok piksel dalam citra hasil enkripsi.

Penelitian ini akan menggali penggunaan Linear Congruential Generator (LCG) sebagai elemen kunci dalam proses pengacakan blok pada metode enkripsi IDEA (International Data Encryption Algorithm) pada citra digital. LCG akan diterapkan sebagai alat utama dalam menghasilkan urutan angka pseudorandom yang akan memengaruhi pengacakan blok sebelum proses enkripsi IDEA dilakukan pada citra digital. Tujuan dari penerapan LCG adalah untuk memperkenalkan tingkat keacakan yang diperlukan dalam urutan blok yang dienkripsi, dengan harapan mengurangi korelasi yang dapat ditemukan pada citra hasil enkripsi. Dalam kerangka penelitian ini, penerapan LCG pada proses pengacakan blok akan menjadi langkah penting dalam menyesuaikan proses enkripsi IDEA pada citra digital. Penggunaan LCG diharapkan dapat mengoptimalkan tingkat keamanan enkripsi dengan mengaburkan pola korelasi yang mungkin muncul pada blok-blok piksel dalam citra hasil enkripsi.

ISSN: 2964-1950

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Tahapan penelitian untuk mengimplementasikan penggunaan Linear Congruential Generator (LCG) dalam enkripsi IDEA pada citra digital dapat terdiri dari beberapa langkah seperti berikut :

Gambar 1. Metode Penelitian

Adapun penjelasan dari setiap tahapan metode penelitian adalah sebagai berikut :

1. Studi Literatur. Menelaah literatur terkait kriptografi, enkripsi citra, IDEA, dan Linear Congruential Generator (LCG) untuk memahami dasar teoritis dan penelitian terdahulu.
2. Perencanaan Penelitian. Menentukan tujuan penelitian, hipotesis, serta batasan-batasan penelitian terkait penggunaan LCG pada enkripsi citra dengan IDEA.
3. Pengumpulan Data. Mengumpulkan dataset citra digital yang akan digunakan untuk uji coba dan eksperimen dan menyiapkan perangkat lunak atau lingkungan kerja yang diperlukan untuk mengimplementasikan algoritma enkripsi IDEA dengan pengacakan menggunakan LCG.
4. Implementasi. Mengimplementasikan algoritma enkripsi IDEA yang menggunakan LCG sebagai pengacakan pada blok citra digital dan melakukan serangkaian pengujian terhadap citra terenkripsi, termasuk analisis keacakkan, evaluasi keamanan, serta analisis kualitas citra hasil enkripsi.
5. Analisis Hasil. Menganalisis hasil dari pengujian dan evaluasi untuk mengevaluasi keefektifan metode pengacakan LCG pada enkripsi IDEA dan menafsirkan hasil-hasil yang diperoleh dan membandingkan dengan tujuan penelitian dan hipotesis yang telah ditetapkan.
6. Kesimpulan. Menyusun kesimpulan dari hasil penelitian, termasuk interpretasi terhadap perbaikan korelasi antar blok pada citra terenkripsi setelah penerapan LCG dan membuat penilaian terhadap kesesuaian hasil dengan tujuan penelitian dan relevansi terhadap kontribusi terhadap keamanan enkripsi citra digital.

2.2 IDEA

IDEA (International Data Encryption Algorithm) adalah algoritma kriptografi yang menjadi subjek perhatian dalam upaya melindungi data secara efektif. Dikembangkan oleh Xuejia Lai dan James Massey pada awal 1990-an, IDEA mengusung konsep enkripsi blok dengan panjang kunci 128-bit yang menjadi landasan keamanan yang kuat [13]. Keunggulan utama IDEA adalah kemampuannya mengenkripsi data dengan cepat dan efisien tanpa mengorbankan tingkat keamanan yang tinggi. Algoritma ini menggabungkan teknik-teknik kriptografi simetris seperti substitusi dan permutasi pada level bit yang menghasilkan operasi enkripsi yang kompleks. IDEA telah menjadi salah satu algoritma kriptografi yang dipercaya dalam berbagai aplikasi, mulai dari keamanan komunikasi hingga perlindungan data sensitif dalam transaksi finansial. Keamanan yang ditawarkan oleh IDEA terutama berakar dari perpaduan proses substitusi dan permutasi yang saling melengkapi dan menghasilkan tingkat keacakan yang tinggi dalam enkripsi data.

ISSN: 2964-1950

Operasi IDEA terdiri dari dua operasi yaitu enkripsi dan dekripsi, adapun tahapan proses enkripsi pada IDEA dapat dijabarkan sebagai berikut :

1. Pembagian Data: Pesan atau blok data yang akan dienkripsi dibagi menjadi blok-blok 64-bit.
2. Inisialisasi Ronda: Enkripsi IDEA terdiri dari beberapa ronda, di mana setiap ronda terdiri dari serangkaian operasi yang terstruktur.
3. Subtitusi Awal (Initial Substitution): Setiap blok 64-bit diubah dengan tabel substitusi awal.
4. Iterasi Ronda: Setiap ronda terdiri dari empat tahapan:
    a. Substitusi Byte: Setiap blok 64-bit dibagi menjadi empat bagian 16-bit. Setiap bagian melewati tabel substitusi byte yang dihasilkan dari kunci enkripsi.
    b. Permutasi (Permutation): Setiap pasangan blok 16-bit diproses melalui permutasi.
    c. Operasi XOR dan Penambahan Modulo (XOR and Modular Addition): Hasil dari tahapan sebelumnya diolah dengan subkunci ronda yang dihasilkan dari kunci enkripsi utama.
    d. Operasi Matriks (Matrix Operations): Hasil dari tahapan sebelumnya dikalikan dalam operasi matriks yang kompleks.
5. Ronda Terakhir dan Output: Setelah ronda terakhir, blok terenkripsi dihasilkan sebagai output.

Sedangkan operasi dekripsi dapat dijabarkan sebagai berikut :

1. Invers Matriks dan Invers Permutasi: Langkah-langkah pada enkripsi dilakukan secara terbalik dalam dekripsi, termasuk invers matriks dan invers permutasi.
2. Invers Substitusi Byte: Tabel substitusi byte yang digunakan dalam dekripsi adalah invers dari tabel yang digunakan pada enkripsi.
3. Penambahan dan XOR: Langkah-langkah ini dilakukan secara terbalik dalam proses dekripsi.
4. Iterasi Ronda: Seperti pada enkripsi, dekripsi juga terdiri dari beberapa ronda dengan operasi yang terbalik.
5. Output: Hasil dekripsi merupakan blok data asli sebelum dienkripsi.

2.3 LCG

Linear Congruential Generator (LCG) adalah salah satu jenis generator angka pseudorandom yang cukup sederhana dan sering digunakan dalam berbagai aplikasi. Metode ini menghasilkan deret angka yang hampir acak dengan mengalikan nilai sebelumnya dengan suatu konstanta, kemudian menambahkan nilai konstan lain, dan diambil modulus dengan suatu bilangan prima besar [14]. Formula umum dari LCG adalah:

$$X_{n+1} = (a\ x\ X_n + c)\ mod\ m \quad (1)$$

2.4 Correlation Coefficient

Korelasi mengacu pada ukuran statistik yang mengukur hubungan linier antara dua variabel. Dalam konteks citra digital, korelasi koefisien digunakan untuk menilai hubungan antara piksel, blok, atau fitur dalam citra. Pemahaman akan korelasi koefisien memungkinkan pengoptimalan dalam proses pemampatan citra, mengidentifikasi dan memanfaatkan redundansi yang ada. Pearson Correlation Coefficient merupakan metrik yang sering digunakan untuk mengukur korelasi antara dua variabel numerik. Dalam konteks citra, koefisien korelasi Pearson sering digunakan untuk mengevaluasi hubungan antar piksel atau blok. Analisis koefisien korelasi telah banyak digunakan pada penelitian sebelumnya untuk menganalisis tingkat keamanan citra hasil enkripsi [15].

$$r = \frac{\sum_{i=1}^{n}(X_i - \hat{X})(Y_i - \hat{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \hat{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \hat{Y})^2}} \quad (2)$$

3. HASIL DAN PEMBAHASAN

Enkripsi pada citra digital melibatkan proses pengolahan blok-blok piksel yang terdiri dari nilai-nilai bilangan yang mewakili warna dan intensitas pada citra. Proses ini menggunakan algoritma kriptografi blok, seperti IDEA, yang dirancang untuk mengubah blok-blok ini secara kriptografis agar tidak dapat dibaca tanpa kunci dekripsi yang tepat. Pada tingkat implementasi, enkripsi IDEA pada citra digital membagi citra menjadi blok-blok piksel dengan ukuran yang ditentukan, misalnya, blok 8x8 piksel. Setiap blok piksel ini dianggap sebagai data yang akan dienkripsi. Setelah membagi citra menjadi blok-blok piksel, setiap blok piksel ini diubah menjadi representasi

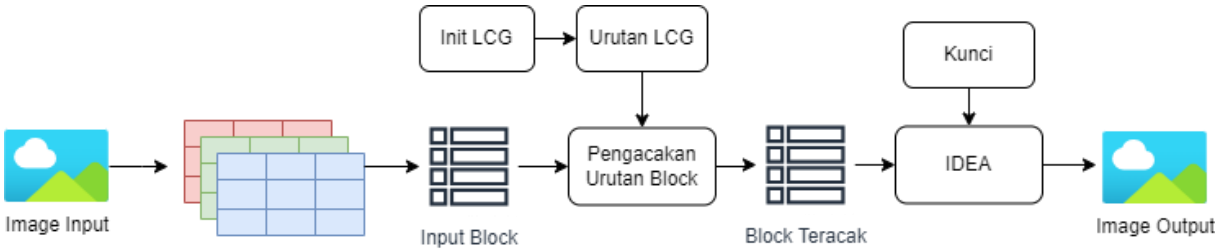
ISSN: 2964-1950

bitnya. Algoritma IDEA kemudian diterapkan pada setiap blok bit ini menggunakan prosedur enkripsi IDEA yang telah dijelaskan sebelumnya.

3.1 Proses IDEA - LCG

Implementasi penggunaan Linear Congruential Generator (LCG) pada proses enkripsi IDEA (International Data Encryption Algorithm) pada citra digital melibatkan penggunaan LCG untuk menghasilkan angka-angka pseudorandom yang digunakan dalam proses pengacakan blok sebelum proses enkripsi dilakukan. Berikut adalah langkah-langkah yang dapat dilakukan dalam implementasi ini:

1. Penentuan Parameter LCG: Langkah pertama adalah menentukan parameter-parameter untuk LCG, seperti nilai awal (seed), konstanta pengali (a), konstanta penambahan (c), dan modulus (m). Pemilihan parameter ini penting untuk menghasilkan deret angka pseudorandom yang memiliki sifat keacakkan yang baik.
2. Generate Deret Angka Pseudorandom: Setelah parameter-parameter LCG ditentukan, proses LCG dimulai dengan menghasilkan deret angka pseudorandom. Deret angka ini akan digunakan sebagai kunci atau pengacakan dalam proses enkripsi blok IDEA pada citra digital.
3. Pengacakan Blok dengan Deret Angka Pseudorandom: Deret angka pseudorandom yang dihasilkan oleh LCG akan digunakan untuk mengacak blok-blok piksel dalam citra sebelum proses enkripsi IDEA dilakukan. Proses ini bertujuan untuk memperkenalkan tingkat keacakan yang diperlukan dalam urutan blok yang akan dienkripsi, sehingga mengurangi pola korelasi yang dapat dimanfaatkan untuk menganalisis citra hasil enkripsi.
4. Enkripsi IDEA setelah Pengacakan Blok: Setelah proses pengacakan blok menggunakan deret angka pseudorandom dari LCG, proses enkripsi IDEA dilakukan pada blok-blok piksel yang telah diacak. Proses ini memanfaatkan kunci enkripsi yang dihasilkan dari proses LCG untuk mengubah blok-blok piksel menjadi bentuk terenkripsi.
5. Iterasi pada Seluruh Blok Citra: Langkah-langkah di atas diulang pada setiap blok piksel dalam citra digital yang akan dienkripsi, sehingga seluruh citra akan melalui proses pengacakan blok dengan LCG dan proses enkripsi IDEA.



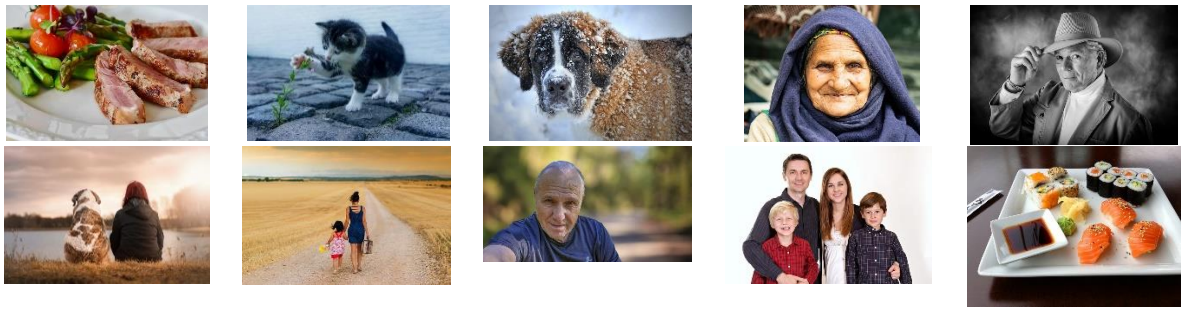
Gambar 2. Proses IDEA – LCG

Langkah pertama adalah menghasilkan deret angka pseudorandom menggunakan LCG dengan parameter-parameter yang telah ditentukan sebelumnya, seperti nilai awal (seed), konstanta pengali (a), konstanta penambahan (c), dan modulus (m). Citra digital yang akan dienkripsi dibagi menjadi blok-blok piksel dengan ukuran tertentu, misalnya, blok piksel berukuran 8x8 atau 16x16. Deret angka pseudorandom yang dihasilkan oleh LCG akan digunakan sebagai kunci pengacakan untuk setiap blok piksel dalam citra. Proses ini mengacu pada urutan atau indeks blok-blok piksel yang akan dienkripsi. Setiap blok piksel akan diacak berdasarkan nilai-nilai pseudorandom yang dihasilkan. Setelah proses pengacakan blok selesai, blok-blok piksel yang telah diacak akan siap untuk proses enkripsi IDEA. Proses enkripsi ini akan menggunakan blok-blok piksel yang telah diacak sebagai masukan untuk menghasilkan citra terenkripsi. Langkah-langkah di atas diulang pada setiap blok piksel dalam citra digital yang akan dienkripsi. Proses pengacakan blok menggunakan deret angka pseudorandom dari LCG dilakukan pada seluruh blok piksel sebelum proses enkripsi IDEA. Proses pengacakan blok dengan LCG bertujuan untuk memperkenalkan tingkat keacakan yang diperlukan pada urutan blok piksel sebelum proses enkripsi dilakukan. Hal ini bertujuan untuk mengaburkan pola korelasi pada hasil enkripsi serta meningkatkan tingkat keamanan enkripsi citra digital.

ISSN: 2964-1950

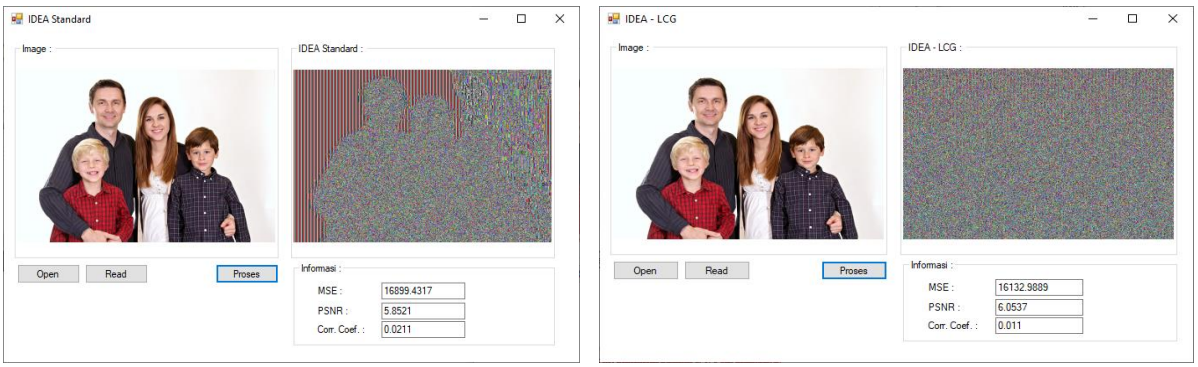
3.2 Implementasi IDEA - LCG

Dalam tahap implementasi, penggunaan dataset citra yang berasal dari OpenDataset menjadi kunci dalam menguji dan mengevaluasi algoritma enkripsi yang telah dikembangkan. Sebanyak 10 citra yang dipilih dari OpenDataset digunakan sebagai sampel representatif untuk proses uji coba. Proses implementasi melibatkan pengolahan citra secara berurutan menggunakan algoritma enkripsi IDEA yang telah diintegrasikan dengan pengacakan blok menggunakan Linear Congruential Generator (LCG). Proses implementasi dilakukan dengan membangun aplikasi berbasis perangkat lunak yang memanfaatkan algoritma enkripsi yang telah dikembangkan. Penggunaan teknologi dalam pengembangan aplikasi memungkinkan implementasi algoritma enkripsi IDEA dengan metode pengacakan menggunakan Linear Congruential Generator (LCG).



Gambar 3. Citra Pengujian

Pertama, dilakukan langkah pengumpulan dataset yang terdiri dari 10 citra yang beragam dalam jenisnya, seperti citra berwarna dan citra grayscale, serta dengan resolusi yang bervariasi. Setiap citra ini diambil dari OpenDataset untuk memastikan keberagaman dan representasi yang lebih baik dalam pengujian. Dalam tahap ini, akan dilakukan enkripsi terhadap 10 citra yang dipilih dari dataset untuk mengevaluasi kinerja algoritma. Untuk memberikan pemahaman yang lebih visual dan jelas terkait hasil implementasi, aplikasi yang telah dikembangkan dapat dilihat pada gambar 4 yang menggambarkan hasil implementasi pengamanan citra digital menggunakan IDEA biasa dan yang menggunakan kombinasi IDEA - LCG.



(a) (b)

Gambar 4. Implementasi IDEA Standard (a) dan IDEA – LCG (b)

3.3 Analisa Hasil

Analisa hasil dilakukan dengan menghitung nilai – nilai indikator yang dapat digunakan untuk mengukur keamanan citra digital hasil enkripsi. Pada penelitian ini, akan dilakukan analisa terhadap indikator MSE, PSNR

ISSN: 2964-1950

dan *Correlation Coefficent* pada enkripsi IDEA standar yang dapat dilihat pada tabel 1 dan enkripsi IDEA yang mengaplikasikan LCG yang dapat dilihat pada tabel 2.

Tabel 1. Hasil Pengujian IDEA Standard

No.	Dataset	MSE	PSNR	Correlation Coefficient
1	dataset1	10097.97	8.0885	-0.0038
2	dataset2	9818.615	8.2103	-0.0102
3	dataset3	9399.082	8.3999	0.0011
4	dataset4	10730.8	7.8245	-0.0036
5	dataset5	10942.61	7.7396	0.0015
6	dataset6	10669.67	7.8493	-0.0025
7	dataset7	8812.838	8.6796	-0.0015
8	dataset8	8338.993	8.9197	-0.001
9	dataset9	16899.43	5.8521	0.0211
10	dataset10	12027	7.3292	-0.0025

Tabel 2. Hasil Pengujian IDEA - LCG

No.	Dataset	MSE	PSNR	Correlation Coefficient
1	dataset1	10075.99	8.0979	-0.0012
2	dataset2	9820.464	8.2095	-0.0006
3	dataset3	9371.691	8.4126	-0.0017
4	dataset4	10703.97	7.8354	-0.0011
5	dataset5	11016.19	7.7105	0
6	dataset6	10681.93	7.8443	0.0003
7	dataset7	8810.504	8.6808	0.0004
8	dataset8	8350.407	8.9137	0.0022
9	dataset9	16134.06	6.0534	0.013
10	dataset10	11968.73	7.3503	0

Hasil pengujian yang dapat dilihat pada tabel 1 dan tabel 2 dapat dilihat perbedaan yang signifikan antara enkripsi citra menggunakan IDEA biasa dan penggunaan IDEA yang didukung dengan Linear Congruential Generator (LCG) dalam hal korelasi koefisien, Mean Squared Error (MSE), dan Peak Signal-to-Noise Ratio (PSNR). Terdapat penurunan signifikan pada Mean Squared Error (MSE) rata-rata sebesar 0.04856 dan juga menunjukkan penurunan kualitas citra dengan nilai PSNR rata-rata sebesar 0.036315195 serta perbaikan koefisien korelasi rata-rata sebesar 4.571596485 ketika menggunakan enkripsi IDEA dengan LCG.

4. KESIMPULAN

Implementasi penggunaan Linear Congruential Generator (LCG) pada proses enkripsi citra dengan IDEA menunjukkan perbedaan yang signifikan dibandingkan dengan enkripsi IDEA biasa dalam hal keamanan dan kualitas citra terenkripsi Penggunaan LCG dalam pengacakan blok pada proses enkripsi citra menghasilkan penurunan signifikan pada nilai korelasi koefisien. Nilai yang mendekati 0 dengan perbaikan koefisien korelasi rata-rata sebesar 4.571596485 menunjukkan minimnya hubungan antar blok piksel dalam citra terenkripsi, mengindikasikan efektivitas pengacakan blok dalam mengaburkan pola korelasi. Terdapat perbaikan yang

signifikan pada koefisien korelasi rata-rata, menandakan bahwa metode pengacakan blok dengan LCG mampu menghasilkan citra terenkripsi yang memiliki pola korelasi yang minim antar blok pikselnya. Ini memberikan tingkat keamanan yang lebih tinggi terhadap serangan kriptanalisis yang memanfaatkan pola korelasi. Dengan demikian, penggunaan LCG pada proses pengacakan blok dalam enkripsi citra dengan IDEA memberikan peningkatan signifikan dalam aspek keamanan dengan pengurangan korelasi yang nyata, meskipun terdapat sedikit pengorbanan pada kualitas citra. Ini menegaskan bahwa metode ini efektif meningkatkan keamanan citra terenkripsi dalam lingkup serangan kriptanalisis yang memanfaatkan pola korelasi, dengan memperhatikan kompromi pada kualitas citra. Meskipun terdapat penurunan Mean Squared Error (MSE) yang mengindikasikan pengurangan distorsi antara citra asli dan terenkripsi, terjadi sedikit degradasi kualitas citra dengan penurunan nilai Peak Signal-to-Noise Ratio (PSNR). Hal ini menunjukkan adanya trade-off antara keamanan dan kualitas citra.

DAFTAR PUSTAKA

[1] M. Gupta, K. K. Gupta and P. K. Shukla, "Session key based fast, secure and lightweight image encryption algorithm," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10391-10416, 2021.

[2] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid and A. Y. Al-Dubai, "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966-12982, 2022.

[3] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855-37865, 2021.

[4] W. Sirichotedumrong, Y. Kinoshita and H. Kiya, " Pixel-based image encryption without key management for privacy-preserving deep neural networks," *Ieee Access*, vol. 7, pp. 177844-177855, 2019.

[5] Y. Pourasad, R. Ranjbarzadeh and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, 2021.

[6] P. K. Naskar, S. Bhattacharyya, D. Nandy and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," *Nonlinear Dynamics*, vol. 100, pp. 2877-2898, 2020.

[7] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, p. 107484, 2020.

[8] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, pp. 1154-1169, 2021.

[9] B. Mondal and T. Mandal, "A secure image encryption scheme based on genetic operations and a new hybrid pseudo random number generator," *Multimedia Tools and Applications*, vol. 79, no. 25-26, pp. 17497-17520, 2020.

[10] C. Yang, I. Taralova, S. El Assad and J. J. Loiseau, "Image encryption based on fractional chaotic pseudo-random number generator and DNA encryption method," *Dynamics*, vol. 109, no. 3, pp. 2103-2127, 2022.

[11] K. Sinha, P. Paul and A. Amritanjali, "An Improved Pseudorandom Sequence Generator and its Application to Image Encryption," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 16, no. 4, pp. 1307-1329, 2022.

[12] S. M. Hardi, R. S. Ramadhani, E. M. Zamzami, J. T. Tarigan and I. Jaya, "Security of Image File with Tiny Encryption Algorithm And Modified Significant Bit Pseudo Random Number Generator," in *In Journal of Physics: Conference Series*, 2020.

[13] M. N. Alenezi, H. Alabdulrazzaq and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," *International Journal of Communication Networks and Information Security*, vol. 12, no. 2, pp. 256-272, 2020.

[14] B. A. Hameedi, A. A. Hattab and M. M. Laftah, "A Pseudo-Random Number Generator Based on New Hybrid LFSR and LCG Algorithm," *Iraqi Journal of Science*, vol. 63, no. 5, pp. 2230-2242, 2022.

[15] Y. Liu, H. Zhang and Q. Wang, "The Role of Correlation Coefficients in Image Encryption," *IEEE Transactions on Image Processing*, vol. 29, pp. 589-601, 2020.