JUIT
ADMI Jurnal Ilmiah Teknik
JUIT Vol 2 No. 1 Januari 2023 | P-ISSN: 2828-6936 E-ISSN: 2828-6901, Page 01-10

HASIL ANALISIS STATISTIK, DIFERENSIAL, DAN KUALITAS CITRA TERHADAP KOMPOSISI LOGISTIC CIRCLE MAP

Makmun
Fakultas Ilmu Komputer, makmun@staff.gunadarma.ac.id, Universitas Gunadarma

ABSTRACT

The problem of data security is still a matter of concern in the digital era like today. An effective security method is needed and it is difficult to break into. Encryption is an effective method of ensuring data security. The encryption algorithm is built using a chaotic cipher base so that performance in securing data and information increases. The new chaotic composition resulting from two chaotic maps will have better randomness. Logistic Map and Circle Map were chosen because they have good randomness. The new chaotic composition is called the Logistic Circle Map (LC Map). By bifurcation diagram test, Lyapunov Exponent, and NIST random test, the best density occurs at X_0=0.9 , K = 1000, r = 3.7 and Ω = 0.4. The new chaotic composition parameters have passed all 16 NIST (National Institute of Standards and Technology) tests. There are four parameters used in this study in order to obtain a sufficiently high key space, namely 1.296 × 〖10〗^84 combinations and having a high level of lock sensitivity of 10−17. The image encryption algorithm of the LC Map function has high resistance against various attacks. This can be proven by carrying out key space tests, sensitivity tests for key spaces, histogram tests, entropy, correlation coefficients, and differential tests using the UACI NPCR. The test results on digital image decryption using the Mean Square Error (MSE) show a result of 0 and the Peak Signal to Noise Ratio (PSNR) shows a result of ∞. That is, the encrypted image is similar to the original image.

Keywords: bifurcation, lyapunov, exponent.

ABSTRAK

Masalah keamanan data masih menjadi hal yang mengkhawatirkan di era digital seperti sekarang ini, Diperlukan metode pengamanan yang efektif dan sulit untuk dibobol. Enkripsi adalah salah satu metode efektif untuk menjamin keamanan data. Algoritma enkripsi dibangun dengan menggunakan basis chaotic cipher agar kinerja dalam pengamanan data dan informasi meningkat. Komposisi chaotic baru yang dihasilkan dari dua chaotic map akan memiliki keacakan yang lebih baik. Logistic Map dan Circle Map dipilih karena memiliki keacakan yang cukup baik. Komposisi chaotic baru itu dinamakan Logistic Circle Map (LC Map). Dengan uji diagram bifurkasi, Lyapunov Eksponen, dan uji keacakan NIST, densitas terbaik terjadi pada X_0=0,9 , K = 1000, r = 3.7 dan Ω = 0.4. Parameter komposisi chaotic baru tersebut telah lolos seluruh uji NIST (National Institute of Standard and Technology) yang berjumlah 16. Ada empat parameter yang digunakan dalam penelitian ini agar mendapatkan ruang kunci yang cukup tinggi yaitu sebesar 1,296 × 〖10〗^84 kombinasi dan memiliki tingkat sensitivitas kunci sebesar 10−17. Algoritma enkripsi citra dari fungsi LC Map memiliki daya tahan yang tinggi terhadap berbagai serangan. Hal ini dapat dibuktikan dengan melakukan uji ruang kunci, uji sensitivitas terhadap ruang kunci, uji histogram, entropi, koefisien korelasi, dan uji diferensial menggunakan NPCR UACI. Hasil pengujian pada dekripsi citra digital dengan menggunakan Mean Square Error (MSE) menunjukkan hasil 0 dan Peak Signal to Noise Ratio (PSNR) menunjukkan hasil ∞. Artinya, citra yang dienkrip memiliki kemiripan dengan citra yang asli.

Kata Kunci: bifurkasi, lyapunov, eksponen.

1. PENDAHULUAN

Ketika dunia menjadi semakin digital, volume data yang masuk semakin meningkat secara eksponensial. International Telecommunication Union (ITU) mencatat, jumlah pengguna internet di dunia mencapai 5,3 miliar orang pada 2022. Ini berarti 66% dari populasi dunia telah menggunakan internet.

Penelitian ini mengkhususkan pada data citra, karena kebocoran data citra terjadi dalam berbagai tempat, mulai dari market place bahkan institusi negara. Transmisi dan berbagi informasi berbasis data digital sering menghadapi masalah pencurian data, penghapusan, dan serangan, yang akan menyebabkan kerugian besar bagi pemilik data digital. Oleh karena itu, keamanan data dan informasi menjadi sangat penting karena data yang disajikan secara digital dapat diakses oleh siapapun. Usaha-usaha yang dapat dilakukan untuk meningkatkan privasi dan kepercayaan adalah dengan menggunakan teknologi kriptografi.

Berdasarkan kunci penyandiannya, kriptografi dibagi menjadi dua jenis yaitu enkripsi kunci simetri dan enkripsi kunci publik. Suatu enkripsi dikatakan enkripsi simetris ketika proses enkripsi dan dekripsinya menggunakan kunci yang sama. Enkripsi publik artinya untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda. [Menezes et al.,1996] Dalam penyimpanan dan pengiriman data atau informasi rahasia terdapat dua tipe serangan, yaitu cryptanalytic attack dan brute force attack [Stallings, 2011]. Serangan tersebut bertujuan untuk memperoleh kunci sehingga dengan mudah memperoleh plaintext dari ciphertext. Cryptanalytic attack mengandalkan sifat dari algoritma dan juga dari karakteristik umum dari plaintext atau beberapa pasang plaintext-ciphertext, sedangkan brute force attack mencoba setiap kemungkinan kunci pada ciphertext sampai plaintext ditemukan.

Dua fungsi chaos yang sudah dikenal menunjukkan sifat chaos adalah Logistic Map dan Circle Map. Keduanya memiliki potensi keacakan yang tinggi. Logistic Map menjadi salah satu map paling terkenal di teorema sistem dinamis dan chaos. Map ini awalnya digunakan untuk menggambarkan pertumbuhan penduduk dunia seiring berjalannya waktu di bawah batasan berdasarkan fungsi kurva berbentuk S yang sangat umum. Dan sekarang Logistic Map dapat digunakan untuk mensimulasikan berbagai proses alam. Fungsi logistik menggunakan diferensial persamaan yang memperlakukan waktu sebagai hal yang berkelanjutan. Logistic Map menggunakan persamaan perbedaan non linier untuk melihat langkah-langkah waktu diskrit.

Circle Map adalah chaotic map satu dimensi yang memetakan sebuah lingkaran ke dirinya sendiri Dalam makalah ini dikembangkan chaotic map baru yang merupakan hasil komposisi dari Logistic Map dan Circle Map. Komposisi yang dihasilkan diharapkan memiliki nilai chaotic yang memiliki nilai random yang tinggi, sehingga bisa dijadikan alternatif baru sebagai chaotic RNG. Dalam pengujian chaotic terhadap fungsi chaos baru yang diperoleh tersebut menggunakan Nilai Lyapunov exponent, Diagram bifurkasi, dan Uji NIST. Sedangkan analisis daya tahan algoritma dilakukan berdasarkan analisis tingkat sensitifitas nilai awal, besarnya ruang kunci, analisis histogram, korelasi, dan entropi, analisis distribusi uniform dari chipper image, dan analisis kualitas citra dengan Peak Signal to Noise Ratio (PSNR).

2. TINJAUAN PUSTAKA

Kriptografi berasal dari bahasa Yunani yaitu kryptos dan graphia. Kriptografi adalah ilmu yang memelajari tentang teknik matematika yang berhubungan tentang aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, dan autentikasi data. Tujuan lain dari kriptografi adalah memberikan layanan integritas data (data integrity) yang menjamin keaslian pesan atau pesan belum pernah dimanipulasi. Otentikasi bertujuan untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi dan mengidentifikasi kebenaran sumber informasi. Anti penyangkalan (non-repudiation) bertujuan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. [Munir, 2006]

Teori chaos menggambarkan perilaku sistem dinamis non linear yang menunjukan fenomena yang kacau. Sistem chaos sangat peka terhadap nilai awal, yang menunjukan hasil yang sangat kacau jika ada perbedaan di awal walaupun sangat sedikit. Map dari suatu nilai tertentu yang polanya sangat sensitif terhadap perubahan disebut Chaotic Map. Fenomena yang umum di dalam teori chaos adalah peka terhadap perubahan nilai awal, yang juga dikenal sebagai ketergantungan yang peka pada nilai. Kepekaan ini berarti bahwa perbedaan kecil pada nilai awal fungsi, misalnya perubahan sebesar 10-100. Setelah fungsi diiterasi sejumlah kali, maka akan dihasilkan perbedaan yang sangat besar pada nilai fungsinya.

Persamaan logistik (Logistic Map) merupakan contoh pemetaan polinomial derajat dua dan seringkali digunakan sebagai contoh bagaimana rumitnya sifat chaos yang dapat muncul dari suatu persamaan yang sangat sederhana. Persamaan ini dipopulerkan oleh seorang ahli biologi yang bernama Robert May pada tahun 1976. Ia menulis makalah yang menarik di Nature tentang Logistic Map. Hal itu memicu revolusi analisis dinamis dan secara bertahap berkembang menjadi luas seperti sekarang ini.

Dan sekarang logistic Map dapat digunakan untuk mensimulasikan banyak proses di alam. Logistic Map juga merupakan satu dimensi yang telah digunakan secara luas dengan definisi sebagai berikut :

$$X + 1 = rX (1 - X) \quad (2.1)$$

Dimana 0<x<1 , yang merepresentasikan populasi pada tahun ke n. Parameter x dapat disebut juga sebagai nilai chaos (0 < x < l). Sedangkan r adalah bilangan postif yang merepresentasikan kombinasi antara

nilai reproduksi dan makanan. Parameter r dapat disebut juga dengan sebutan laju pertumbuhan ($0 < r < 4$).

Circle Map didefinisikan dengan persamaan berikut.[Boyland,1986]

$$x_{n+1} = x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n) \bmod 1 \quad (2.2)$$

Mod 1 menunjukkan bagian desimal dari sebuah angka, sehingga nilai map selalu lebih rendah dari 1 tetapi tidak kurang dari 0, dan parameter Ω, K ∈ R, Ω terdapat pada interval $0 \leq \Omega \leq 1$, karena ini adalah suku penjumlahan tunggal dalam modulo 1 ini, jadi semua nilai Ω lainnya telah diwakili oleh interval ini. Circle Map menunjukkan sifat yang sangat menarik karena memiliki potensi kekacauan yang tidak terbatas. Saat nilai K menjauh dari 0, Lyapunov exponentnya terus meningkat, meskipun mungkin turun di beberapa titik dan kenaikannya melambat.

Sistem chaos sudah banyak digunakan di dalam pembangkitan bilangan acak. Barisan bilangan acak dibangkitkan dari iterasi terhadap fungsi chaos berdasarkan sebuah nilai awal dan satu atau lebih parameter. Karakteristik yang paling penting dari sistem chaos adalah peka terhadap nilai awal; yaitu jika dua nilai awal dipilih sangat dekat satu sama lain, maka setelah sejumlah iterasi tertentu, barisan nilai yang dihasilkannya akan berbeda secara signifikan. Sifat peka semacam ini sangat berharga untuk algoritma kriptografi [Munir, 2006].

Definisi fungsi yaitu sebuah fungsi f adalah suatu aturan padanan yang menghubungkan tiap obyek x dalam satu himpunan, yang disebut daerah asal, dengan sebuah nilai unik f(x) dari himpunan kedua. Himpunan nilai yang diperoleh secara demikian disebut daerah hasil (jelajah) fungsi tersebut (Purcell dan Varberg, 1998).

Uji Keacakan Key Stream dilakukan dengan uji statistik yang terdiri dari 16 uji. National Institute of Standards and Technology (NIST) test adalah tes statistika yang dilakukan untuk menguji keacakan bilangan yang dibangkitkan oleh Random Number Generator (RNG) dan Pseudorandom Number Generator (PRNG) yang digunakan dalam kriptografi. Tes ini terdiri atas 16 rangkaian tes yang menguji keacakan bilangan yang dibangkitkan oleh RNG atau PRNG sehingga dapat diketahui kelayakan untuk diaplikasikan dalam kriptografi. Pada penelitian ini, PRNG yang akan membuat barisan bit adalah Logistic Chaotic Map (LC Map).

3. METODOLOGI PENELITIAN

Langkah-langkah pada tahapan penelitian ini adalah:

1. Melakukan pengembangan fungsi chaos baru yang didapatkan dari komposisi fungsi Logistik Map dan Circle Map.
2. Menguji sifat chaotic fungsi chaos baru melalui diagram bifurkasi dan lyapunov exponent, serta menguji keacakan key stream yang dibangkitkan dari fungsi chaos baru menggunakan uji NIST.
3. Merancang algoritma enkripsi citra digital berdasarkan fungsi chaos baru.
4. Membuat aplikasi enkripsi dan dekripsi citra digital menggunakan bahasa pemrograman Python.
5. Melakukan simulasi dan uji coba program aplikasi enkripsi dan dekripsi menggunakan data uji berupa citra warna dan citra greyscale.
6. Melakukan analisis kinerja algoritma enkripsi citra digital berbasis fungsi chaos baru berdasarkan: analisis tingkat sensitifitas nilai awal, besarnya ruang kunci yang digunakan, analisis histogram, korelasi, dan entropi, analisis distribusi uniform dari chiper-image, serta analisis kualitas citra hasil enkripsi dan dekripsi dengan PSNR..

4. HASIL DAN PEMBAHASAN

4.1 Perancangan Fungsi

Dalam disertasi ini, fungsi chaos baru dirumuskan melalui proses komposisi dua fungsi chaos yaitu Logistic Map dan Circle Map seperti yang ditunjukkan pada gambar 3.2. Proses komposisi dua fungsi chaos tersebut dapat dilakukan karena keduanya memiliki derajat dan dimensi yang sama. Fungsi Logistic Map dinyatakan sebagai $f(x)$. Sedangkan fungsi Circle Map dinyatakan sebagai $g(x)$. Maka fungsi chaos baru LC Map dinyatakan sebagai $h(x)$, yaitu:

Fungsi Logistic Map

$f(x) = xn+1 = r\,xn\,(1 - xn)$ (4.1)

Fungsi Circle Map

$$g(x) = x_{n+1} = \left(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)\right) m \quad 1 \quad (4.2)$$

Dikomposisikan

$(f \circ g)(x) =$

Untuk $0 \leq x \leq 1$ $= x_{n+1} = r\,xn\,(1 - xn)$

Untuk $0 \leq x \leq 1$ $g(x) = x_{n+1} = \left(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)\right) m \quad 1$

$$h(x) = (f \circ g)(x) = f\left(g(x)\right)$$

$$= r\left(x + \Omega + \frac{K}{2\pi}\sin(2\pi\ )\, m \quad 1\right)\left(1 - \left(x + \Omega + \frac{K}{2\pi}\sin(2\pi\ )\right) m \quad 1\right) \quad (4.3)$$

Jadi didapatkan fungsi rekursif adalah:

$$x_{n+1} = r\left(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)\, m \quad 1\right)\left(1 - \left(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)\right) m \quad 1\right) \quad (4.4)$$

Untuk selanjutnya fungsi komposisi Logistic Map dan Circle Iterated Map akan digunakan sebagai pembangkit *key stream* dalam proses enkripsi dan dekripsi.

4.2 Lyapunov Exponent

Lyapunov Exponent (LE) adalah nilai untuk menggambarkan sistem kekacauan (Alan Wolf, et al., 1985) dan didefinisikan sebagai perbedaan eksponensial divergensi atau konvergensi dua vektor di sebuah bidang yang mengukur nilai dari divergensi atau konvergensi tersebut dari dua titik awal yang sangat dekat dari sistem dinamika. LE berfungsi untuk menganalisis perilaku dinamika dalam suatu sistem, apakah chaos, limit, atau periodikal.

Jika X adalah sebuah kumpulan, maka pemetaan $: X \rightarrow X$ dikatakan chaotic di X, jika f sensitif pada suatu kondisi awal. f memiliki topologi transitif dan periodenya rapat.

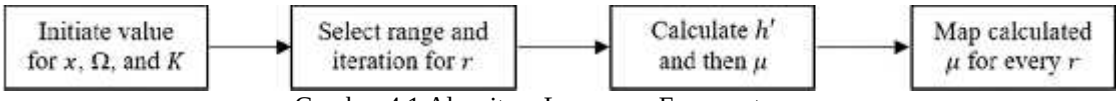
Untuk sembarang fungsi, Lyapunov Exponent didefinisikan sebagai:

$$\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln\left|(f^i)'(X_0)\right| \quad (4.5)$$

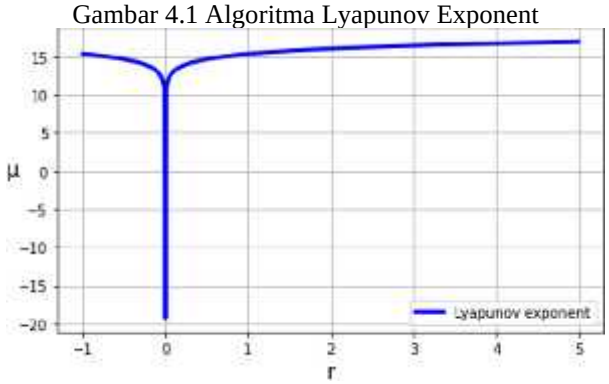
Dengan komposisi fungsi baru yaitu LC Map maka Lyapunov Exponentnya adalah sebagai berikut:

$$h^r(x) = r\left[1 - 2x + \left(K \quad (2\pi\ )\right)\left[1 + 2\Omega + 2\left(\frac{K}{2\pi}\sin(2\pi\ )\right)\right]\right] \quad (4.6)$$

Menurut kajian literatur, sebuah fungsi dikatakan chaotic jika ia memiliki nilai Lyapunov Exponent yang positif. Untuk mendapatkan sifat chaotic, harus ada LE positif . Jadi, jika ada satu LE positif maka gerakannya akan chaotic. (Weifeng Shi, 2006) Gambar 4.1 menunjukkan algoritma dari Lyapunov Exponent. Pertama, masukkan nilai $x, K, r, d \quad \Omega$. Parameter nilai tersebut sesuai dengan nilai yang sudah ditentukan yaitu: $x_0 = 0.9$, $K = 1000$ and $\Omega = 0.4$. Langkah selanjutnya adalah memilih interval dan iterasi untuk r. Kemudian, hitunglah h' dan μ. Terakhir, map akan mengkalkulasi μ untuk setiap r



Gambar 4.1 Algoritma Lyapunov Exponent

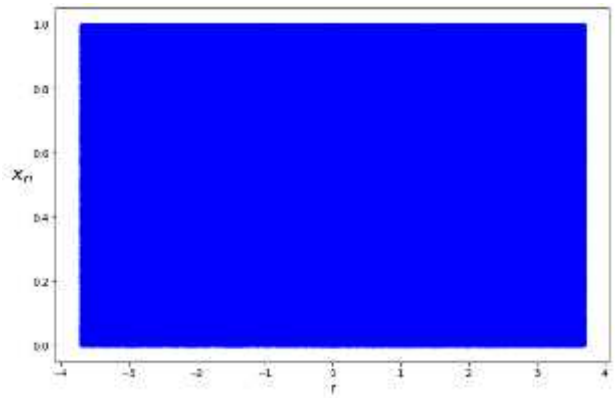


Gambar 4.2 Diagram Lyapunov Exponent dari LC Map

Seperti yang terlihat pada gambar 3.4, untuk r □ $[-1,0)$ □ $(0,5]$, LC map menunjukkan nilai lyapunov exponent yang positif. Artinya, LC Map memiliki nilai chaotic dalam interval tersebut. Dari perhitungan lyapunov exponents dan diagram bifurfasi di atas, r yang digunakan pada sistem ini adalah $r \neq 0$.

4.3 Diagram Bifurkasi

Diagram bifurkasi adalah diagram dalam dinamika nonlinier, yang menunjukkan kemungkinan nilai jangka panjang dari sebuah sistem (kesetimbangan/titik tetap atau orbit periodik) suatu sistem sebagai fungsi dari suatu parameter. Menurut Kocarev, bifurkasi adalah perubahan kualitatif dalam variabel parameter dari sistem dinamis.



Gambar 4.3 Diagram Bifurkasi LC Map dengan $X_0 = 0.9$

Dari gambar diagram bifurkasi LC Map di atas, dapat dilihat bahwa dengan $X_0 = 0.9$ dan $r = 3.7$ terlihat hasil yang padat. $r \in [-4,0) \cup (0,4]$. Nilai tersebut akan digunakan sebagai nilai kunci untuk menghasilkan key stream fungsi LC Map.

4.4 Pengujian Keacakan Key Stream dengan NIST

Tes ini diberikan untuk meratakan keacakan urutan bilangan yang dihasilkan oleh peta LC seperti dalam persamaan. NIST Test Suite adalah paket statistik yang berisi 16 tes yang dikembangkan untuk menguji keacakan urutan biner (Rukhin, 2010). Tabel 1 menunjukkan hasil yang diperoleh untuk LC map. Pada tes ini, nilai r yang digunakan adalah 3.7.

Tabel 4.1. Hasil Uji Randomness Test NIST dari LC Map

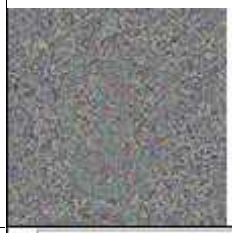
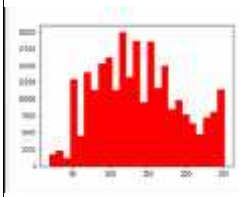
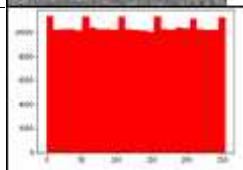
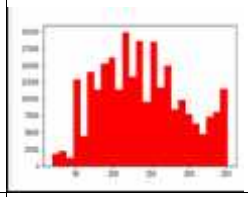
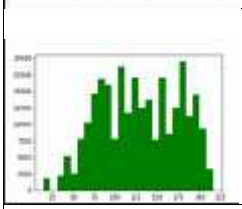
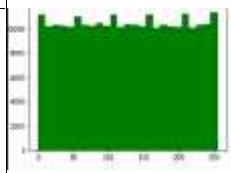
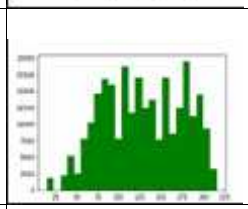
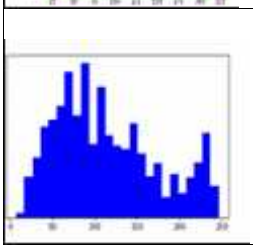
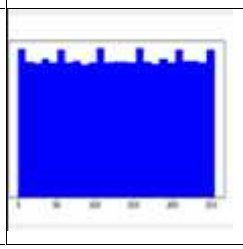
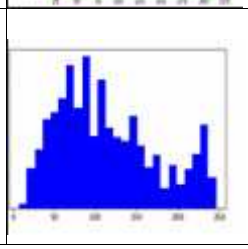
Type of Test	P-Value	Conclusion
Frequency Test (Monobit)	0.421396	Random
Frequency Test within a Block	0.637244	Random
Run Test	0.610999	Random
Longest Run of Ones in a Block	0.103734	Random
Binary Matrix Rank Test	0.141656	Random
Discrete Fourier Transform (Spectral) Test	0.847186	Random
Non-Overlapping Template Matching Test	0.297797	Random
Overlapping Template Matching Test	0.583725	Random
Maurer's Universal Statistical Test	0.239610	Random
Linear Complexity Test	0.347975	Random
Serial Test	0.025477	Random
	0.078958	Random
Approximate Entropy Test	0.716084	Random
Cummulative Sums (Forward) Test	0.530576	Random
Cummulative Sums (Reverse) Test	0.681092	Random
Random Excursions Test	0.508979[a]	Random
Random Excursions Varian Test	0.477982[a]	Random

Tabel 4.1 menunjukkan bahwa LC chaos map memenuhi seluruh NIST randomness test. Dengan demikian, LC Map memiliki nilai sempurna untuk RNG yaitu 100% hasilnya adalah random untuk x_0 = 0.9, K = 1000, r = 3.7 and Ω = 0.4

4.5 Sensitivitas Kunci

Pengujian sensitivitas kunci pada LC Map akan dilakukan dengan menggunakan nilai kunci yang berbeda dengan kunci yang digunakan pada proses enkripsi. File citra yang digunakan adalah file citra baboon dengan ukuran 512×512 piksel. Hasil deskripsi akan ditampilkan pada tabel 4.3 dengan menggunakan nilai parameter kunci yang sama dengan proses enkripsi, yaitu $X_0 = 0.9, r = 3.7, \Omega = 0{,}4, K = 1000, it = 100$. Tabel 4.2 menampilkan bentuk histogram dengan komponen citra red, green, dan Blue (RGB).

Tabel 4.2 Hasil Deskripsi menggunakan kunci yang sama dengan proses enkripsi

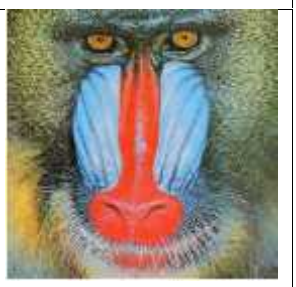
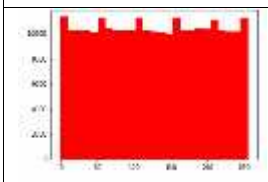
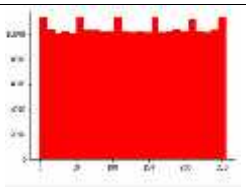
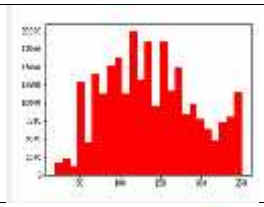
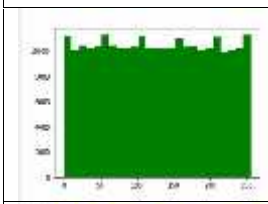
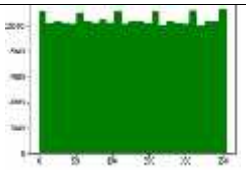
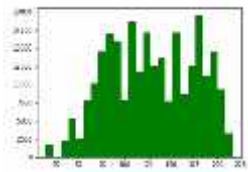
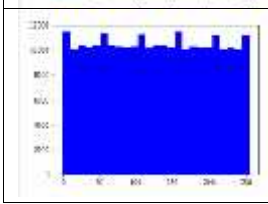
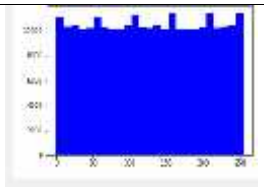
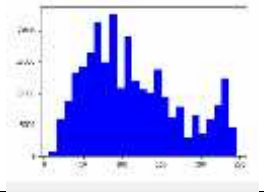
Citra Asli	Citra Enkripsi	Citra Dekripsi
		
		
		
		

Proses deskripsi yang dilakukan dengan parameter chaos yang memiliki kunci sama sesuai tabel 4.4 dapat mengembalikan citra terenkrip menjadi citra asli. Citra terenkrip memiliki histogram yang cenderung datar dimana secara statistik memiliki distribusi relatif yang uniform. Dengan hasil yang sama antara histogram citra asli dan citra terenkrip bak itu citra red, green, maupun blue, membuktikan bahwa algoritma dekripsi berhasil mengembalikan cipher image menjadi citra asli.

Kemudian, dengan kunci yang berbeda pada proses enkripsi, akan dilakukan proses dekripsi per masing-masing parameter untuk mengetahui analisis sensitivitasnya. Ada variasi tiga nilai kunci yang berbeda dan akan diujikan pada masing-masing parameter, yaitu terhadap nilai awal X_0, nilai parameter r, nilai parameter Ω, dan nilai parameter K.

Tabel 4.3 pada kolom pertama akan menyajikan data hasil proses dekripsi menggunakan selisih nilai 10^{-6} terhadap nilai X_0 pada proses enkripsi. Dari gambar terlihat citra dengan selisih nilai 10^{-6} masih belum memiliki perubahan bentuk. Pengujian kedua menggunakan selisih nilai 10^{-1} sebagaimana tampak pada kolom dua. Selisih tersebut masih belum membuat citra Kembali menjadi citra asli. Hingga terakhir, digunakan angka 10^{-1} . Pada selisih nilai 10^{-1} citra asli baru dapat diperoleh kembali. Saat selisihnya mencapai 10^{-1} usaha dekripsi berhasil mendapatkan informasi citra aslinya. Hal itu menunjukkan bahwa dua bilangan ini yaitu 0,9 dan 0,90000000000000001 dianggap bilangan yang sama yakni 0,9. Diperlihatkan usaha mendekrip dengan menggunakan kunci yang berbeda untuk citra uji coba mulai dari 10^{-6} sampai 10^{-1} . Sehingga didapatkan sensitivitas kunci dari algoritma ini adalah sampai 10^{-1}

Tabel 4.3 Hasil Uji sensitivitas untuk Perbedaan Awal X_0

$X_0 = 0.9 + 10^{-6}$	$X_0 = 0.9 + 10^{-1}$	$X_0 = 0.9 + 10^{-1}$
		
		
		
		

4.6 Ukuran Ruang Kunci

Serangan brute force dilakukan dengan mencoba semua kemungkinan kunci saat mendekrip agar didapatkan citra yang asli. Agar peluang berhasilnya serangan brute force minimal, maka algoritma harus memiliki ruang kunci yang besar. Ruang kunci menyatakan jumlah total kunci yang berbeda yang dapat digunakan untuk melakukan enkripsi/dekripsi (Fu, Chen, Zou, Meng, Zhan & Yu 2012). Algoritma enkripsi L C Map menggunakan lima parameter kunci, yaitu X_0, r, K, dan Ω dan iterasi dengan domainnya ialah: $X_0 \in (0, 9)$, $r \in \{(3,7)\}$, $\Omega \in (0,4)$, $K \in$ R, dan iterasi $\in$ Z. Dengan demikian ruang kunci seluruhnya adalah

$$(R \quad k \quad X_0) \times (R \quad k \quad r) \times (R \quad k \quad K) \times (R \quad k \quad \Omega)$$
$$= (10^{1}) \times (4 \times 10^{1}) \times (1{,}8 \times 10^{3}) \times (10^{1}) \times (1{,}8 \times 10^{1})$$
$$\approx 12{,}96 \times 10^{372}.$$
$$\approx 1{,}296 \times 10^{373}$$

4.7 Analisis Statistik

Analisis statistik terhadap algoritma dilakukan untuk melihat daya tahan algoritma terhadap serangan statistik (*statistical attack*). Analisis ini mencakup analisis histogram dan analisis korelasi. antara dua peubah acak. Nilai-nilai piksel pada citra terenkripsi tersebar merata atau uniform dapat ditunjukkan secara statitik pada dengan menggunakan uji Goodness of fit. Tingkat keabuan piksel ada pada nilai 0-255 yang dijadikan sebagai banyaknyakelas yaitu 256 kelas. Derajat bebasnya adalah 256 - 1 = 255, dan level signifikannya adalah 1%, nilai kritis adalah ≈ 310.457. Terlihat dari hasil percobaan yang ditunjukkan pada Tabel 4.4 semua nilai statistik uji < nilai kritis. Maka dapat disimpulkan semua data yang diuji tersebut terbukti terdistribusi uniform.

Tabel 4.4: Hasil Uji Statistik Data Citra Warna

Data	Nilai Uji Statistik		
	Red	Green	Blue
1	207.937	260.769	231.693
2	232.492	272.132	291.223
3	283.548	274.956	265.713
4	281.941	255.351	229.367
5	253.567	233.189	269.180
6	303.269	281.622	224.999
7	240.795	264.741	271.721
8	246.615	287.392	291.236
9	302.337	302.337	302.337

Korelasi adalah ukuran yang menyatakan kekuatan hubungan linier antara dua peubah acak (Munir 2012). Koefisien korelasi artinya korelasi dari dua variabel diskrit yang masing-masing beranggotakan n elemen. Pada citra asli piksel-piksel yang bertetangga memiliki hubungan linier yang kuat ditandai dengan nilai koefisein korelasi yang tinggi yaitu mendekati+1 atau -1. Pada citra terenkripsi piksel-piksel yang berteta Perhitungan korelasi dalam hal ini ditunjukkan terhadap data uji ke-1 yaitu data uji Baboon.bmp dengan ukuran 512 × 512 piksel. Hasil perhitungan koefisien korelasi citra asli dan citra terenkripsi dapat dilihat pada Tabel 4.5

Tabel 4.5: Perbandingan Koefisien Korelasi antara Dua Piksel Bertetangga pada Data Citra Warna

Koefisien Korelasi	RGB	Horizontal	Vertikal	Diagonal
Citra Asli	R	0.91844	0.86029	0.84005
	G	0.88380	0.79648	0.76403
	B	0.92344	0.87729	0.85478
Citra Terenkripsi	R	0.91844	0.86029	0.84005
	G	0.88380	0.79648	0.76403
	B	0.92344	0.87729	0.85478

Dapat dilihat pada Tabel 4.5 bahwa nilai koefisien korelasi citra asli warna merah (red), hijau (green), dan biru (blue) secara horizontal, vertikal, dan diagonal adalah sama dengan citra terenkripsi

Perhitungan korelasi citra keabuan (greyscale) dilakukan terhadap data uji ke-14 yaitu data uji village.png dengan ukuran 1024 × 1024 piksel. Hasil perhitungan koefisien korelasi citra asli dan citra terenkripsi dapat dilihat pada Tabel 4.6

Tabel 4.6: Perbandingan koefisien korelasi dua piksel bertetangga pada data citra greyscale

Koefisien Korelasi	Horizontal	Vertikal	Diagonal
Citra Asli	0.96776	0.95539	0.94798
Citra Terenkripsi	0.96776	0.95539	0.94798

Dapat dilihat pada Tabel 4.6 bahwa nilai koefisien korelasi citra asli secara horizontal, vertikal, dan diagonal adalah sama dengan citra terenkripsi.

4.8 Analisis Diferensial

Untuk menguji seberapa besar perbedaan antara dua citra terenkripsi ketika terjadi perubahan satu bit pada citra asli, dapat diketahui dengan melakukan ana isis diferensial. Analisis diferensial dapat diukur dengan menggunakan The Number of Changing piksel Rate (NPCR) dan The Unified Averaged Intensity (UACI). NPCR untuk mengetahui presentase jumlah piksel citra terdekripsi berubah ter- hadap citra aslinya. Sementara UACI untuk melihat presentase nilai perbedaan antara citra terenkripsi dan citra asli. Hasil perhitungan NPCR dan UACI ditunjukkan pada Tabel 4.7

Tabel 4.7: Nilai NPCR dan UACI citra terenkripsi saat citra asli mengalami perubahan 1 bit.

Data	NPCR (%)	UACI(%)	Data	NPCR (%)	UACI (%)
1	99.5	29.79	10	99.5	27.94
2	99.5	29.59	11	99.6	27.79
3	99.5	29.47	12	99.6	27.44
4	99.5	32.86	13	99.5	32.32
5	99.5	32.93	14	99.5	32.37
6	99.6	33.01	15	99.5	32.45
7	99.5	32.58	16	99.5	28.78
8	99.5	32.45	17	99.5	28.23
9	99.6	32.61	18	99.5	28.80

4.9 Analisis Kualitas Citra

Analisis kualitas citra dilakukan antara citra asli dengan citra hasil dekripsi yang dilakukan untuk melihat apakah citra terdekripsi sama atau menyerupai citra aslinya atau tidak. Penilaian iu akan melihat apakah algoritma enkripsi dan dekripsi dapatberfungsi sebagaimana yang diharapkan. Analisis kualitas citra dilakukan dengan menggunakan Peak Signal to Noise Ratio (PSNR). Pada penelitian ini, signal yang dimaksud adalah nilai intensitas piksel dari citra asli. Sedangkan noise yang dimaksud adalah apabila pada saat dekripsi ada perubahan nilai intensitas piksel. Sedangkan Mean Square Error (MSE) yang dimaksud adalah error yang terjadi pada saat dekripsi. Adapun proses enkripsi dan dekripsi dilakukan secara statis terhadap data uji citra. Hasil untuk data uji citra warna dan untuk data uji citra greyscale disajikan pada Tabel 4.8

Tabel 4.8: Hasil Uji MSE dan PSNR Citra Warna dan Greyscale

Data	MSE	PSNR	Data	MSE	PSNR
1	0	∞	10	0	∞
2	0	∞	11	0	∞
3	0	∞	12	0	∞
4	0	∞	13	0	∞
5	0	∞	14	0	∞
6	0	∞	15	0	∞
7	0	∞	16	0	∞
8	0	∞	17	0	∞
9	0	∞	18	0	∞

Berdasarkan hasil pada Tabel 4.8 diperoleh kesimpulan bahwa untuk setiapdata uji didapat nilai MSE=0 dan nilai PSNR=∞. Hal tersebut mempunyai arti bahwa citra hasil dekripsi sama dengan citra aslinya.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan yang merujuk pada perumusan masalah dapat ditarik kesimpulan sebagai berikut:

1. Fungsi chaos baru yaitu, LC Map yang dikembangkan dengan menggunakan komposisi antara dua fungsi chaos Logistik Map dan Circle Map.
2. Fungsi LC Map setelah melalui uji lyapunov exponent, uji bifurkasi diagram dan uji kerandoman dengan NIST terbukti memenuhi syarat properti chaos. Selanjutnya fungsi ini digunakan untuk membangkitkan key stream yang di gunakan dalam proses enkripsi dan dekripsi.
3. Key stream yang dibangkitkan oleh Fungsi LC Map berupa barisan bilangan byte yang memiliki nilai acak dalam rentan 0 dan 255. Jumlah byte key stream yang dibangkitkan sama dengan jumlah byte data yang akan dienkripsi. Proses enkripsi yang dilakukan adalah menggunakan model enkripsi substitusi XOR byte per byte. Fungsi MSC Map memiliki 4 parameter, sehingga berdasarkan pada hasil perhitungan, fungsi ini dapat menghasilkan ruang kunci sebesar 12.96×10372 , sehingga algoritma ini susah diserang dengan brute force attack.
4. Pengujian serangan pada data citra terenkripsi menggunakan statistical attack dan differential attack menunjukkan bahwa metode yang diusulkan memiliki daya tahan tinggi. Selain itu, uji akurasi terhadap hasil dekripsi citra meng- gunakan perhitungan MSE dan PSNR menunjukkan 100% tepat sama dengan data citra aslinya (nilai MSE = 0 dan PSNR = ∞).

DAFTAR PUSTAKA

[1] Menezes, A. J. (2018), Van Oorschot, P. C. & Vanstone, S. A., Handbook of applied cryptography, CRC press,
[2] P. Stallings, W. (2014) , Cryptography and network security, 4/E, Pearson Education India
[3] Boyland, P. L. (1986) 'Bifurcations of circle maps: Arnol'd tongues, bistability and rotation intervals', Communications in Mathematical Physics 106(3), 353–381,
[4] Munir, R (2006), 'Kriptografi. bandung', Informatika 1(7).,
[5] Varberg D, Purcel E and Rigdon KS (1998), Calculus (9th Edition) PDF
[6] Wolf A, et al., (1985), Determining Lyapunov exponents from a time series,
[7] Kocarev L and Lian S, (2011) , Chaos-Based Cryptography: Theory, Algorithm and Applications, Berlin: Springer-Verlag.
[8] Andrew Rukhin, Juan Soto, et.all, (2010), A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22 Revision 1a,
[9] Fu, C., Chen, J.-j., Zou, H., Meng, W.-h., Zhan, Y.-f. & Yu, Y.-w. (2012), 'A Chaos-based digital image encryption scheme with an improved diffusion strategy', Optics express 20(3), 2363–2378,
[10] Munir, R. (2012), 'Analisis keamanan algoritma enkripsi citra digital menggunakan kombinasi dua chaos map dan penerapan teknik selektif', Jurnal Ilmiah Teknologi Informasi 10(2), 89–95.