IMPLEMENTASI ALGORITMA ENKRIPSI CITRA DIGITAL BERBASIS CHAOS MENGGUNAKAN FUNGSI KOMPOSISI LOGISTIC DAN GAUSS ITERATED MAP

Suci Boru Kembaren[1)], Suryadi[2),] Triswanto [3)]
[1]Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadarma
email: suci_k@staff.gunadarma.ac.id
[2]Departemen Matematika, Universitas Indonesia
email: yadi.mt@sci.ui.ac.id
[3]Fakultas Teknologi Industri, Universitas Gunadarma
Email :triswanto.1995@gmail.com

Abstract

Computer and information technology is very fast as technology develops. People can easily use the internet as a media for searching, sending and receiving information. Information can be in the form of text, image, audio, video, and multimedia, information can be quickly spread throughout the world through the internet. To increase the durability of the algorithm used in the encryption process from brute force attacks, one of them is by implementing chaos theory. The aim of the study was to create a digital image encryption algorithm based on chaos function. The chaos function used is the result of the composition of the Logistic Map function and the Gauss Map function. The chaos function will be used to generate a key stream that will be used to substitute the original image pixel into an encrypted image with XOR operations. The simulation results show that the key sensitivity of this algorithm is that up to 10^{-16} and the key space is the key is 1.8×10^{79}. The NIST test was performed and proved that the resulting key stream was random, and from the histogram test the pixel value of the uniform encryption image. This shows that the digital image encryption algorithm with the Log-gauss Map function is resistant to brute force and statistical attacks. PSNR test results for all original images with the results of the description of the same pixel values .

Keywords: *Enkripsi, Chaos, Citra digital, Kriptografi, Log-gauss Map, Logistic Map, Gauss Iterated Map*

1. PENDAHULUAN

Perkembangan teknologi komputer dan informasi sangat cepat seiring berkembangnya teknologi, dalam hal ini internet yang merupakan bagian dari teknologi komputer dan informasi juga ikut berkembang dengan cepat. Internet merupakan media yang paling berpengaruh dalam proses komunikasi dan bertukar informasi bagi masyarakat. Sekarang ini dengan mudah masyarakat dapat menggunakan internet sebagai media pencarian, pengiriman, dan penerima informasi. Informasi dapat berupa berupa teks, citra, audio, video, dan multimedia, informasi dapat cepat tersebar di seluruh dunia memalui internet. Dalam hal ini aspek keamanan data dan informasi merupakan hal yang perlu diperhatikan.Khususnya untuk informasi yang bersifat pribadi yang memiliki nilai yang tinggi untuk dijaga kerahasiaannya.

Dalam melakukan pengiriman dan penyimpanan data atau informasi perlu dilakukan pengamanan agar terhindar dari resiko terhadap penyadapan dan pencurian.Hal ini agar data atau informasi yang ada di dalamnya tidak mudah diketahui oleh pihak-pihak yang tidak

memiliki hak terhadap data atau infomasi tersebut. Oleh karena itu, dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau informasi yang dikenal dengan istilah kriptografi dengan cara melakukan enkripsi data.

Berbagai macam teknik enkripsi citra digital telah diusulkan demi meningkatkan keamanan dan efisiensi.Salah satu teknik enkripsi citra digital yang diusulkan adalah teknik enkripsi berbasis chaos.Metode ini memberikan kombinasi yang baik antara kecepatan, keamanan yang tinggi, kompleksitas, dan daya komputasi.

Penelitian terus dilakukan untuk meningkatkan daya tahan algoritma yang digunakan pada proses enkripsi dari serangan brute force, salah satunya dengan cara mengimplementasikan teori chaos. Algoritma yang mengimplementasikan teori chaos adalah algoritma Logistic Map dan Gauss Iterated Map. Beberapa penelitian yang menerapkan algoritma tersebut dalam kriptografi adalah "Image encryption using chaotic logistic map" oleh N. K. Pareek, Vinod Patidar, dan K. K. Sudab, "Digital Sound Encryption with Logistic Map and Number Theoretic Transform" oleh Yudi Satria, P.H. Gabe Rizky and Suryadi MT, "Performance of Chaos-Based Encryption Algorithm for Digital Image" oleh Suryadi MT, Eva Nurpeti serta "Gauss Iterated Map Based RGB Image Encryption Approach" oleh Ajita Sahay and Chittaranjan P radhan dan "Image Encryption based on Random Scrambling and Chaotic Gauss Iterative Map" oleh Marutesh Chandra Sharma dan Pankaj Sharma. Algoritma mengimplementasikan teori chaos dengan membangkitkan deret bilangan yang bersifat acak yang sensitif akan nilai awal dan ergodicity.

Berdasarkan uraian diatas, penulis melakukan usaha untuk menemukan fungsi chaos baru dan terinspirasi untuk melakukan penelitian tentang keamanan data dengan mngimplementasikan fungsi komposisi dari algoritma Logistic Map dan Gaussian Map pada proses enkripsi dan dekripsi citra digital. Hal tersebut diharapkan dapat meningkatkan ketahanan terhadap serangan bruteforce dan statistical attack.

2. KAJIAN LITERATUR

Kriptografi berasal dari Bahasa Yunani, crypto dan graphia.Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan dari pengirim dan disampaikan kepada penerima secara aman tanpa mengalami gangguan dari pihak ketiga [Schneier, 1996]..

Teori chaos berasal dari teori system yang memperlihatkan kemunculan tidak teratur, meskipun sebenarnya teori ini digunakan untuk menjelaskan kemunculan data acak.

Chaos adalah tipe dari perilaku suatu sistem ataupun fungsi yang bersifat acak, peka terhadap nilai awal dan ergodicity. Fungsi yang memiliki sifat chaos dinamakan fungsi chaos. Fungsi chaos sudah dibuktikan sangat cocok untuk merancang sarana untuk proteksi data [Kocarev, 2011].

Logistic Map adalah pemetaan polynomial derajat 2 disebut juga sebagai contoh pola dasar kompleksitas. Perilaku acak atau kacau dapat muncul dari persamaan dinamik non-linear yang sangat sederhana. Logistic Map dipopulerkan pada akhir 1976 dalam jurnal oleh ahli biologi Robert May, sebagai bagian dari model demografi diskrit waktu yang dianalogikan dengan persamaan logistic, yang pertama kali diciptakan oleh Pierre Francois Verhulst. Fungsi Logistic Map didefinisikann sebagai fungsi satu variabel x dan r parameter tetap. Nilai variabel x_0 dalam interval (0, 1), x_n untuk n = 0,1,2,3,... dan r dalam interval (0, 4]. n merupakan isi inisial iterasi, secara sistematis Logistic Map ditulis seperti berikut [Kocarev, 2011]:

$$X_{n+1} = rXn\,(1 - Xn) \qquad (1)$$

Gauss Iterated Map dikenal sebagai peta nonlinear mengulangi dari real ke interval nyata yang diberikan oleh fungsi Gauss Map [1]:

$$\boldsymbol{x_{n+1} = exp(-a\,x_n^2) + \beta} \quad (2)$$

Dimana a dan b merupakan parameter yang disebutkan sebagai Gauss Iterated Map.Parameter a dan b terkaid dengan lebar dan tinggi dari representasi kurva gaus. Meskipun perilaku Gauss Iterated Map sama seperti Logistic Map, akan tetapi dinamika yang terkait map ini lebih komplikasi seperti mengandung dua parameter. Padahal sebagian besar fitur dari Logistic Map juga menyajikan di Gauss Iterated Map tetapi fitu-fitur tertentu dari Gauss Iterated Map seperti periode tidak berlipat ganda dan stabilitas yang tidak di perlihatkan sama sekali oleh Logistic Map .

Fungsi Komposisi

Tinjau fungsi-fungsi dengan domain dan kodomainnya berupa himpunan bagian dari bilangan real. Ada beberapa nama fungsi seperti fungsi konstan linear, kuadrat atau fungsi polinom, fungsi nilai mutlak, fungsi trigonometri, fungsi logaritma, fungsi eksponen dan lain sebagainya. Bila kita memiliki sebuah himpunan fungsi, maka kita dapat melakukan operasi penjumlahan, pengurangan,perkalian dan pembagian pada fungsi-fungsi itu[Rosen,2011]. Misalnya $f(x) = x^2$ dan $g(x) = 2$, maka $f(x) + g(x) = (f + g)(x) = x^2 + 2$, $f(x) - g(x) = (f - g)(x) = x^2 - 2$, $f(x).g(x) = (f.g)(x) = x^2.2 = 2x^2$ dan $\frac{f(x)}{g(x)} = \left(\frac{f}{g}\right)(x) = \frac{x^2}{2}$.

Operasi XOR

Suatu proposisi adalah suatu pernyataan (statement) yang memiliki nilai kebenaran true (benar, T) atau false (salah, F) tetapi tidak keduanya pada saat dinyatakannya.

Jika p dan q adalah proposisi maka eksklusif or dari p dan q adalah sebuah proposisi juga. Nilai kebenaran dari p XOR q adalah benar pada saat p dan q memiliki nilai kebenaran yang berbeda, dan salah apabila p dan q memiliki nilai kebenaran yang sama [Rukhin,2010].

Komputer merepresentasikan informasi dalam bit-bit. Suatu bit memiliki 2 kemungkinan nilai, yaitu 0 dan 1. Kata “bit” berasal dari binary digit, karena 0 dan 1 merupakan digit-digit yang digunakan dalam merepresentasikan bilangan biner. Operasi XOR berlaku umum untuk bit string yang disebut dengan bitwise XOR. Operasi bitwise XOR menggunakan bit 1 untuk menggantikan true dan bit 0 untuk menggantikan false. Operasi bitwise XOR dari dua bit string dengan Panjang sama adalah sama dengan operasi XOR tipa bit yang bersesuaian. Operasi bitwise XOR dilambang dengan ‘$\oplus$’.

Operasi Modulo

Operator modulo (mod) merupakan unary operator yang memetakan bilangan bulat ke dalam himpunan bilangan bulat {0,1,2,…,d-1}. Misalkan a adalah sebuah bilangan bulat dan d adalah sebuah bilangan bulat positif. Notasi a mod d merupakan sisa dari pembagian a oleh d [3].

3. METODE PENELITIAN

Guna mencapai tujuan penelitian yang telah ditetapkan tersebut maka dilakukan langkah – langkah penelitian sebagai berikut:

1. Studi kepustakaan mengenai kriptografi, teori chaos, algoritma Logistic Map, algoritma Gauss Iterated Map, citra digital.
2. Memformulasikan fungsi baru dengan menerapkan fungsi komposisi pada fungsi chaos Logistic Map dan Gauss Iterated Map.
3. Menguji sifat chaos fungsi dengan lyafunov exponent dan bifurkasi diagram
4. Merancang dan membuat algoritma enkripsi berdasarkan fungsi komposisi tersebut pada data citra digital dan
5. Mengimplementasikan algoritma dengan baik melalui simulasi program enkripsi dan dekripsi citra digital berdasarkan data uji yang diujikan dengan pemrograman Matlab
6. Analisa hasil uji coba pada citra digital baik secara kuantitatif maupun kualitatif

4. HASIL PENELITIAN

4.1 Perancangan Fungsi

Berdasarkan pada persamaan (1) fungsi Logistic Map adalah sebagai berikut:

$$x_{n+1} = r x_n (1 - x_n)$$

Serta Berdasarkan pada persamaan (2) fungsi Gauss Iterated Map adalah sebagai berikut:

$$x_{n+1} = \exp(-a\, x_n^2) + \beta$$

Dengan memegang pada aturan fungsi komposisi, dibuat fungsi komposisi dari fungsi *Logistic Map* dan *Gauss Iterated Map* sebagai berikut:
Diasumsikan bahwa:

$f(x) = x_{n+1} = r x_n (1 - x_n)$

$g(x) = x_{n+1} = \exp(-a\, x_n^2) + \beta$

Maka didapatkan operasi fungsi komposisi untuk $f \circ g$ sebagai berikut:

$$f \circ g = f(g(x)) = r(\exp(-ax^2) + \beta)(1 - (\exp(-ax^2) + \beta)$$

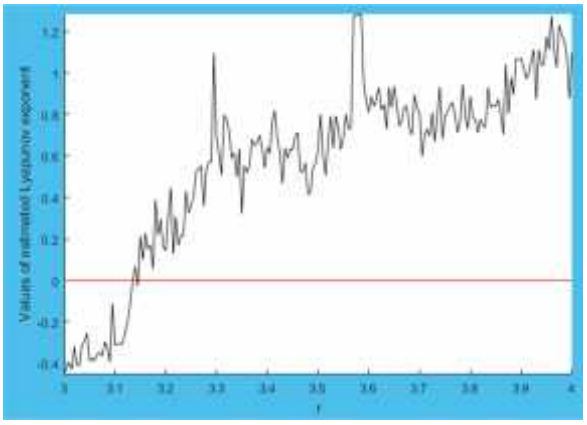
Jadi, didapatkan fungsi iterasi:

$$x_{n+1} = r(\exp(-ax_n^2) + \beta)(1 - (\exp(-ax_n^2) + \beta)) \quad (3)$$

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

4.2 Lyapunov Exponent

Diberikan nilai parameter untuk fungsi Log-gauss Map
$x0 = 0{,}7, r = 3{,}4,\ a = 4{,}2,\ b = 0{,}2$ dan $iterasi = 200$.

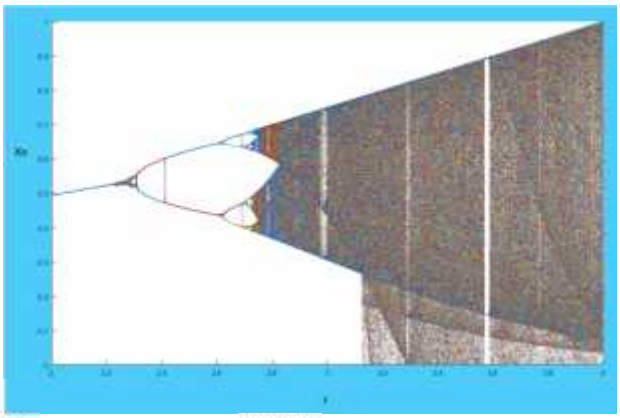


Gambar 1.Lyapunov Exponent Log-gauss Map

Sebuah grafik dari persamaan *Lyapunov exponent* yang mampu mengukur sifat sensitivitas terhadap nilai awal secara kuantitatif.Nilai *Lyapunov* yang bernilai positif menunjukan bahwa persamaan tersebut memiliki sensitivitas tinggi terhadap nilai awal.Terlihat pada Gambar 1.bahwa*Log-gauss Map* tidak bersifat sensitif terhadap nilai awal saat $r \leq 3{,}175$ karena menghasilkan nilai *Lyapunov* negatif. Dapat dilihat pula bahwa yang menghasilkan sifat sensitif terhadap nilai awal adalah saat $r \geq 3{,}175$.

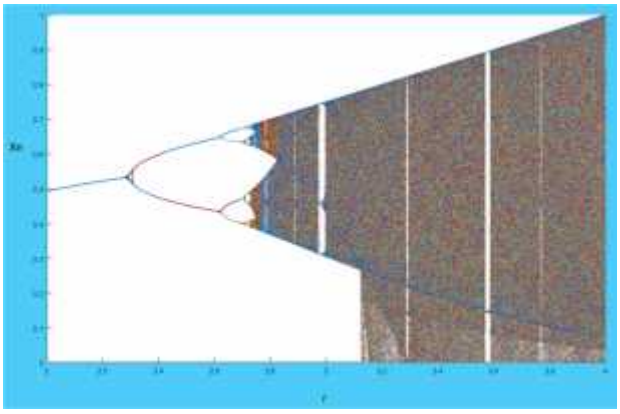
4.3 Diagram Bifurkasi

Disimulasikan diagram bifurkasi dari *Log-gauss Map* dengan bantuan komputer. Pada Gambar 2. nilai awal x_0 yang dipakai adalah 0,7, $a = 4{,}2$, dan $b = 0{,}2$ kemudian di plot hasil pemetaan dari *Log-gauss Map* dimulai dari iterasi 1 sampai 50 untuk tiap – tiap nilai r.



Gambar 2.Bifukasi diagram Log-gauss Map iterasi ke 200

Nilai awal x_0 yang dipakai adalah 0,7 dan di plot hasil pemetaan Log-gauss Map setelah iterasi ke-300 untuk tiap-tiap nilai r.Seperti terlihat pada Gambar 3.



Gambar 3.Bifukasi diagram Log-gauss Map iterasi-300

4.4 Algoritma

Berikut ini adalah langkah-langkah proses enkripsi citra digitalmenggunakan fungsi chaos Log-gauss map :

1. Input kunci $(x0, r, a, b)$ dan citra asli $(M \times N)$.
2. Iterasikan fungsi chaos *Log-gauss map* sebanyak N kali.
3. Iterasikan kembali fungsi chaos Log-gauss Map sebanyak N sehingga menghasilkan barisan bilangan acak $x_i = \{x_1, x_2, x_3, \ldots, x_{n-1}\}$. Sampai nilai i memenuhi nilai n.
4. Iterasikan nilai x_i dan simpan dalam c kemudian absolutkan.
5. Lakukan perkalian setiap nilai c_j dengan 1000. Lakukan pembulatan terhadap nilai c tadi dan lakukan operasi mod untuk nilai c agar menghasilkan Ki. Kemudian lakukan operasi bit XOR untuk Pi dengan Ki, simpan sebagai image output.
6. Proses deskripsi sama saja dengan proses enkripsi karena menggunakan operasi XOR, yang membedakan hanyalah citra yang dimasukkan untuk proses deskripsi adalah citra yang telah di enkripsi.

4. 5 Waktu Enkripsi dan Dekripsi

Hasil uji coba citra warna bahwa semakin besar ukuran citra secara pixel dan kb maka waktu enkrip dan dekripnya semakin besar.Tapi waktu rata-rata enkrip dan dekrip untuk semua ukuran tidak jauh berbeda, seperti hasil pada tabel 3.

Tabel 3. Waktu Proses pada Citra Warna

Nama Citra	Ukuran citra (*pixel*)	Ukuran citra (kb)	Rata-rata Waktu Enkripsi (detik)	Rata-rata Waktu Dekripsi (detik)
Lena.bmp Grey	112 × 112	13.622	0,017019	0,016779
	512 × 512	263.222	0,276364	0,276964
	1230 × 1230	1516.44	1,579340	1,588760
	2600 × 2600	6761.08	7,582808	7,554080
Lena.bmp	112 × 112	37,6860	0,015899	0,017020

Nama Citra	Ukuran citra (*pixel*)	Ukuran citra (kb)	Rata-rata Waktu Enkripsi (detik)	Rata-rata Waktu Dekripsi (detik)
Warna	512 × 512	786,486	0,283048	0,277196
	1230 × 1230	4541,21	1,594860	1,629940
	2600 × 2600	20280,1	7,869260	7,730860

Waktu enkripsi dan dekripsi citra semakin tinggi ukuran resolusinya akan semakin lama pula proses enkripsinya karena dilakukan operasi setiap pixel, semakin banyak pixel maka semakin lama pula proses enkripsi dan dekripsi berlangsung. Waktu enkrip dan dekrip citra warna lebih lama dibandingkan dengan citra grey walaupun ukuran pixel sama, karena ukuran Kb tidak sama.

4.6 Sensitivitas Kunci

Saat selisihnya mencapai 10^{-17}usaha dekripsi berhasil mendapatkan informasi citra aslinya. Hal itu menunjukkan bahwa dua bilangan ini yaitu 0,7 dan 0,70000000000000001 dianggap bilangan yang sama yakni 0,7. Diperlihatkan usaha mendekrip dengan menggunakan kunci yang berbeda untuk citra uji coba mulai dari 10^{-2}sampai 10^{-17}. Sehingga didapatkan sensitivitas kunci dari algoritma ini adalah sampai 10^{-16}.

4.7 Ukuran Ruang Kunci

Pembangkit bilangan acak yang digunakan untuk menghasilkan key stream atau kunci adalah *Log-gauss Map* yang merupakan fungsi komposisi dari *Logistic Map* dan *Gauss Map* dimana fungsinya adalah *Logistic Map* dilanjut dengan *Gauss Map* didapatkan fungsi yang terdapat pada persamaan (3).

Adapun nilainya adalah nilai awal $x_0$dengan parameter nya r, α, β dan I sebagai nilai iterasi.Dengan masing-masing nilai adalah bilangan real dan I adalah bilangan integer. Jika digunakan level presisi yang lebih tinggi, dimisalkan *64-bit double precision* maka dari standar IEEE level presisinya akan mencapai 10^{-15}dan di dalam Matlab tipe data integer memiliki nilai yang mungkin adalah $2^{64} = 1.8 \times 10^{19}$ Maka besar ruang kuncinya adalah $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 1.8 \times 10^{19} = 1.8\,x\,10^{79}$

4.8 Analisis Keacakan

- ***Monobit Test***

1. $n = 64000$
2. $S_n = 8$
3. $S_{obs} = \frac{|8|}{\sqrt{6400}} = 0{,}1$
4. $P_{-value} = erfc\left(\frac{0{,}1}{\sqrt{2}}\right) = erfc(0.0707106781)$

$P_{-value} = 0{,}920344325467$

Sehingga dapat disimpulkan bahwa dengan *significance level* 1% terbukti benar bahwa barisan tersebut random karena $P{-}value > 0.01$.

- **Runs Test**

1. $n = 6400$

2. $\pi = \frac{\sum_j \varepsilon_j}{n} = \frac{3204}{6400} = 0.500625$
3. $\tau = \frac{2}{\sqrt{6400}} - 0{,}025$
4. $V_n(obs) = 3229$
5. $P_{-value} = 0{,}468374636995$

Sehingga dapat disimpulkan bahwa dengan significance level 1% terbukti benar bahwa barisan tersebut random karena $P{-}value > 0.01$.

Didapatkan dari analisis keacakan bahwa key stream yang dihasilkan dari algoritma ini benar-benar acak.

4.9 Histogram dan Goodness of fit

Berdasarkan analisis histogram, diperoleh hasil bahwa nilai-nilai piksel dari citra terenkripsi tersebar secara uniform. Oleh karena itu, dapat dikatakan bahwa cipher-image dari algoritma ini akan sulit dipecahkan dengan statistical attack jika menggunakan sifat statistik yang ada pada citra terenkrip karena nilai piksel tersebar secara merata.

Tabel 4. Nilai Statistik Citra Warna dan Grey

Nama Citra	Ukuran (*pixel*)	Nilai Uji Statistik			
		R	G	B	GREY
Lena.bmp	112 × 112	265,4693	255,061	299,959	276,040816
	512 × 512	272,8203	240,095	267,494	197,429687
	1230 × 1230	266,8203	264,513	269,347	261,916975
	2600 × 2600	305,7833	301,402	274,157	240,392800

4.10 PSNR

Hasil analisis PSNR menunjukkan nilai MSE yang kecil atau 0 dan menghasilkan nilai PSNR tak hingga atau besar, dapat disimpulkan jika citra asli dengan citra hasil dekripsi memiliki nilai-nilai pixel yang sama dalam citra asli dengan citra hasil dekripsi sama atau tidak berubah.

5. SIMPULAN

a. Diperoleh fungsi chaos yaitu *Log-gauss Map* yang merupakan fungsi komposisi dari fungsi *Logistic Map* dan *Gauss Iterated Map*. *Log-gauss Map* pada algoritma enkripsi berbasis chaos. Persamaan Log-gauss Map sebagai berikut:

$$x_{n+1} = r(\exp(-ax_n^2) + \beta)\left(1 - (\exp(-ax_n^2) + \beta)\right)$$

b. Enkripsi dilakukan dengan menggunakan operator XOR sehingga proses dekripsinya dapat dilakukan. Algoritma dan program aplikasi enkripsi telah diimplementasikan pada citra digital, dengan pengujian terhadap 12 data uji citra grayscale dan warna dengan variasi ukuran.

c. Kinerja Algoritma :
   - Waktu proses enkripsi dan dekripsi citra grayscale relatif lebih cepat daripada citra warna. Waktu proses enkripsi dan dekripsi juga bergantung pada ukuran *pixel* dari citra.
   - Algoritma enkripsi memiliki ruang kunci sebesar $1.8\,x\,10^{79}$ karena memiliki 5 parameter / nilai awal dan sensitivitas kunci yang mencapai 10^{-16}, sehingga algoritma ini sangat sulit dipecahkan dengan *brute force attack*.

- Analisis histogram diperoleh hasil bahwa nilai-nilai piksel dari citra terenkripsi tersebar secara *uniform* atau merata dan dari uji *goodness of fit* dihasilkan nilai statistik ujinya < nilai kritis, bahwa *cipher-image* dari algoritma ini akan sulit dipecahkan dengan *statistical attack*.
- *Keystream* yang dihasilkan terbukti benar-benar acak hasil uji NIST yaitu uji monobit dan uji runs. Dengan hasil P_{value} sebagai berikut:
  Hasil Uji Monobit → $P_{value} = 0{,}920344325467 > 0.01$
  HasilUji Runs → $P_{value} = 0{,}468374636995 > 0.01$

d. Hasil uji PSNR terhadap semua citra asli dengan citra hasil dekripsi menujukkan bahwa nilai PSNR tak hingga, dan MSE bernilai nol, hal ini menunjukan bahwa citra asli dengan citra hasil dekripsi sama atau tidak berubah.

Penelitian selanjutnya agar algoritma diuji keacakan terhadap kinerja algoritma ini, dengan standar pengujian internasional NIST yaitu 15 uji keacakan.

6. REFERENSI

Chandra Sharma, Marutesh. Sharma, Pankaj. Image Encryption based on Random Scrambling and Chaotic Gauss Iterative Map. International Journal of Computer Applications. Vol 157 – No 3,(2017) pp. 0975 – 8887

Firmansyah A. ,Dasar-dasar Pemrograman Matlab. IlmuKomputer.com, 2007

Herstein. Abstract Algebra (3rd ed.). Prentice Hall, 1996

Iqbal, Muhammad,Dasar Pengolahan Citra Menggunakan Matlab. Bogor: Marine Instrumentation, 2009

Kocarev, L., & Lian, S , Chaos-based Cyrptography. Berlin Heidelberg : Springer-Verlag, 2011

MT, Suryadi. Nurpeti, Eva. Widya, Dhian. (2014). Performance of Chaos-Based Encryption Algorithm for Digital Image. Telecommunication, Computing, Electronics and Control. Vol.12, No.3,(2014), pp. 675-682.

Pareek, N.K. Patidar, Vinod. Sud, K.K.,Image Encryption Using Chaotic Logistic Map. Image and Vision Computing. 24, pp. 926–934, 2006

Patidar, V., Pareek, N. K., Sud, K. K. , A New Subtitution-diffusion Based Image Chiper Using Chaotic Standard And Logistic Maps. Journal of Communication , Computing and Networking Technologies (ICSCCN) 2011, pp. 364-369.

Purcell, Edwin J., & Varberg, Dale., Calculus with Analitic Geometry, 5th Edition. Jakarta : Erlangga, 1987

Rosen, K.H. , Discrete mathematics and its applications (7th ed.). New York : McGraw-Hill, 2011

Rukhin, Andrew., et. al., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication , (2010), 800-22, revision 1a.

Sahay, Ajita. P radhan, Chittaranjan., Gauss iterated map based RGB image encryption approach. International Conference on Communication and Signal Processing (ICCSP), 2017

Sarmah, Hemanta Kr. Das, Mridul Chandra. Baishya, Tapan Kr. Paul, Ranu. , Characterising Chaos in Gaussian Map. published in International Journal of Advanced Scientific and Technical Research (IJAST), (2016), Vol. 1, pp. 160-172.

Satria, Yudi. Rizky P.H, Gabe. MT, Suryadi., Digital Sound Encryption with Logistic Map and Number Theoretic Transform. International Conference on Mathematics: Pure, Applied and Computation. J. Phys.: Conf. Ser. 974 012016., 2018

Schneier, B., Applied Cryptography : Protocol, Algorithms, and Source Code in C. New York : John Wiley & Sons, Inc,1996

Siringoringo, Rimbun. , Analisis Psnr Pada Steganografi Least Significant Bit Dengan Pesan Terenkripsi Advanced Encription System. METHODIKA. Vol. 2 No. 1, ISSN : 2442-786.,2016

Tan, Xiaoheng. et al. ,New Image Encryption Algoritm Based on Cascade Chaos System. Journal of Information & Computational Science, 11:8, 2467–2478.,2014

Walpole, Ronald E., Introduction to Statistics. Singapore : Prentice Hall International, 1997

Zhang, G., & Liu, Q., A novel image encryption method based on total shuffling scheme. Optics Communications, 284, 2775–2780, 2011