p-ISSN: 2301-5373
e-ISSN: 2654-5101

Enkripsi Gambar Berdasarkan Modifikasi Bit Piksel Dengan Menggunakan Perpaduan Logistic Map Dan Henon Map

I Kadek Aldy Oka Ardita[a1], Agus Muliantara [a2], I Gusti Ngurah Anom Cahyadi Putra [a3], Ngurah Agus Sanjaya ER [a4], Ida Bagus Made Mahendra [a5], I Wayan Supriana [a6].

[a]Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jl. Raya Kampus Unud, Indonesia
[1]aldy.ardita@gmail.com, [2]muliantara@unud.ac.id, [3]anom.cp@unud.ac.id,
[4]agus_sanjaya@unud.ac.id, [5]ibm.mahendra@unud.ac.id, [6]wayan.supriana@unud.ac.id

Abstract

Data theft using malware attacks in this digital era can attack smartphones and cloud servers, in 2018 there was the theft of photos belonging to Aryono Huboyo Djati. Theft can be prevented by applying cryptographic techniques. The purpose of this study was to determine the ability to combine Logistic Map and Henon Map in image encryption and decryption. These two theories were chosen because they are sensitive, with a small change in the input value will have a very significant impact on the output value. First step is changing the image into a matrix and randomizing using the Logistic Map algorithm and then continuing with the XOR process for each pixel bit using the Henon Map algorithm. in this study the encrypted image obtained an average MSE value exceeding 400 and the average PSNR value less than 10dB, this indicates that the cipher image is different from the plain image, and the decryption results show the average MSE value is 0 and the average PSNR value average is 100, this indicates that there is no difference between the description image and the original image.

Keywords: *Image Processing, Cryptography, Logistic Maps, Henon Map, Chaos Theory*

1. Pendahuluan

Seiring dengan berkembangnya infrastruktur dan popularitas media internet saat ini dapat memancing kemunculan hacker. Badan Siber dan Sandi Negara (BSSN) menyatakan pada semester pertama 2021 terdapat lebih dari 741.000.000 serangan yang terjadi, serangan yang paling banyak dilakukan adalah malware. serangan malware merupakan serangan yang ditujukan untuk melakukan pencurian data, manipulasi data, dan merusak data [1], tidak hanya menyerang device komputer pada zaman ini para hacker juga mengembangkan malware untuk menyerang smartphone dan server awan (cloud server). malware dapat dimanfaatkan untuk pencurian data citra juga sudah umum terjadi salah satu kasus yang ditemukan dalam artikel kompasiana.com pada 9 Agustus 2018, foto milik Aryono Huboyo Djati. Digunakan oleh delapan media online di Indonesia tanpa izinnya. Dengan terjadinya kasus diatas dapat diketahui bahwa peningkatan keamanan citra sangat diperlukan untuk menghindari pencurian citra digital, pengamanan citra dapat dilakukan dengan ilmu kriptografi dan steganografi, kriptografi merupakan bidang ilmu yang ditujukan untuk mengamankan citra dari pencurian dengan cara merubah citra asli (plain image) menjadi citra yang sukar untuk dikenali (cipher image), sedangkan steganografi merupakan metode untuk melakukan watermarking atau penyisipan pesan tersembunyi pada suatu citra digital, metode steganografi kurang cocok dalam mengamankan citra digital [2], steganografi melakukan penyisipan pesan ke dalam citra dengan melakukan perubahan nilai bit piksel tertentu hal ini lebih cenderung untuk melakukan pembuktian keaslian pemilik citra [3]. Dari pemaparan tersebut dapat diketahui untuk metode pengamanan citra dari pencurian akan lebih baik menggunakan teknik kriptografi.

Dalam melakukan penerapan teknik kriptografi hal yang sangat penting ialah metode dalam menentukan bilangan secara acak (random number generator), dengan metode penentuan bilangan acak yang baik akan didapatkan citra yang semakin sukar untuk dikenali [4], metode yang cocok dalam

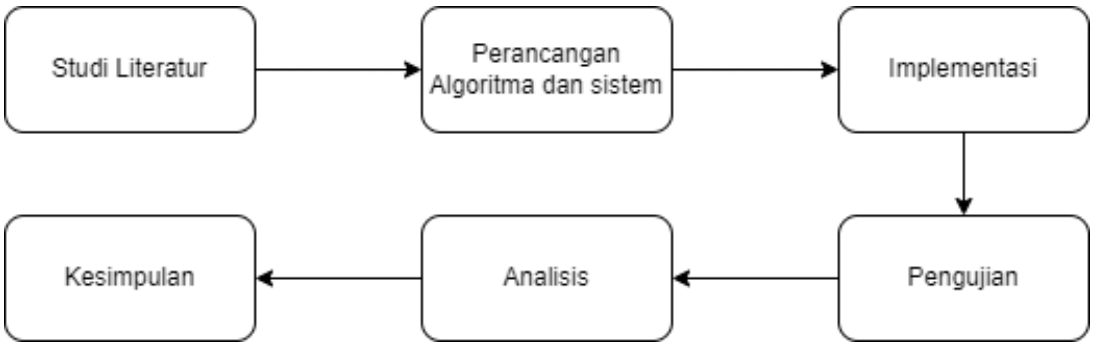
dalam menentukan bilangan acak adalah teori Chaos (Chaos Theory), dalam metode ini terdapat beberapa fungsi yang dapat digunakan dalam melakukan enkripsi citra adalah Logistic Map, Henon Map, dan Arno Cat Map (ACM) teori Logistic Map dapat membangkitnya kunci acak secara terus menerus [5]namun kriptografi berbasis Logistic Map memiliki kekurangan, ruang kunci yang terbilang kecil hingga dapat mengakibatkan mengurangi tingkat keamanan [4].

Algoritma ACM (Arno Cat Map) adalah algoritma untuk melakukan pertukaran posisi antara tiap Piksel pada citra hingga tiap iterasinya akan menghasilkan gambar yang acak, kekurangan yang dimiliki ACM dengan melakukan iterasi secara terus menerus akan dapat mengembalikan citra acak ke citra aslinya [6], selain dapat di dekripsi dengan cara menjalankan algoritma ACM terus menerus ACM juga hanya dapat mengenkripsi citra berdimensi N x N.

Henon Map dapat digunakan dalam melakukan enkripsi, Henon Map dapat memunculkan angka acak sehingga dapat digunakan untuk mendapatkan nilai acak, Henon Map yang merupakan salah satu teori dalam teori Chaos yang memiliki kepekaan terhadap nilai awal yang diberikan, keunggulan teori ini adalah hasil dari perhitungan Henon Map menghasilkan dua nilai acak yang sama sekali tidak dapat diprediksi. Dengan penjelasan diatas penulis memilih teori Logistic Map sebagai pengacak piksel citra digital dengan dikombinasi fungsi Henon Map sebagai metode dalam melakukan pembangkit dua nilai acak sehingga citra makin sukar untuk dikenali.

2. Metode Penelitian

Proses penelitian diawali studi literatur, dengan pengumpulan data citra, perancangan algoritma kriptografi, implementasi algoritma pada sistem, uji sistem, analisis, kesimpulan. Untuk mengetahui kemampuan enkripsi menggunakan *Logistic Map* dan *Henon Map* dilakukan perbandingan nilai MSE dan PSNR yang dihasilkan oleh perpaduan *Logistic Map* dan *Henon Map* dengan nilai MSE dan PSNR yang dihasilkan oleh enkripsi citra menggunakan *Logistic Map*, Tahapan penelitian dapat dilihat pada Gambar 1.



Gambar 1. Desain Umum Penelitian

2.1 Studi Literatur

Teori Chaos adalah sebuah teori dinamis yang menunjukan fenomena chaos atau kacau [7]. Teori Chaos memiliki kepekaan terhadap nilai masukan yang akan mengakibatkan perubahan signifikan pada hasil perhitungannya [8]. Dengan memanfaatkan teori ini proses untuk melakukan penentuan bilangan acak akan mudah untuk dilakukan. Teori Chaos dapat dimanfaatkan sebagai penentu bilangan acak (Random Number Generator), dalam bidang kriptografi kepekaan terhadap perubahan kunci sanga berguna dalam melakukan proses kriptografi itu sendiri. Terdapat metode dalam teori chaos, diantaranya adalah *Logistic Map* dan *Henon Map*.

a. *Logistic Map*
Logistic Map adalah salah satu metode dalam teori chaos yang memiliki bentuk persamaan yang paling sederhana dapat dilihat pada persamaan 1:

$$x_{n+1} = rx_n(1 - x_n) \quad (1)$$

Keterangan :
x_n : nilai awal yang memiliki rentang nilai 0 sampai dengan 1
r : memiliki nilai rentan 0 sampai dengan 4
n : jumlah perulangan ke-n

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Persamaan diatas akan menunjukan nilai acak saat memiliki nilai r > 3.75 dan pada saat r bernilai sama dengan 4 akan didapatkan nilai acak yang tidak dapat diprediksi lagi [6]. Pada persamaan ini nilai awal adalah kunci rahasia yang dimasukan, pada metode ini dengan melakukan sedikit perubahan pada nilai awal akan merubah barisan nilai acak yang dihasilkan. Untuk mendapatkan nilai yang benar-benar tidak berpola pada setiap iterasinya dapat digunakan nilai r = 3.8 dan nilai x_n sebagai kunci dengan syarat x_n kurang dari 1 dan lebih besar dari 0 agar nilai dari x_(n+1) tidak bernilai negatif.

b. *Henon Map*

Sistem kacau memiliki banyak sifat unik seperti ketidakpastian dan sensitivitas keadaan awal [9]. Persamaan yang digunakan dalam Henon Map ditampilkan pada persamaan 1 dan 2:

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

$$y_{n+1} = b\, x_n \quad (3)$$

Keterangan:
x_n : nilai titik awal untuk (x)
y_n : nilai titik awal untuk (y)
a : nilai parameter a
b : nilai parameter b
n : jumlah perulangan ke-n

Untuk persamaan yang bersifat kanonikal, titik awal yang digunakan akan mendekati kumpulan titik yang dikenal sebagai strange attractor Henon, dimana kumpulan titik tersebut mengarah ke bilangan tak terbatas. Sebagai sistem yang bersifat dinamis persamaan Henon memiliki orbitnya sederhana paling sederhana dari persamaan lain, dalam persamaan ini dapat digunakan 1,4 sebagai nilai dari parameter a dan 0.3 digunakan sebagai nilai dari parameter b.

Nilai tersebut digunakan dengan tujuan mendapatkan nilai yang acak di tiap perulangan dari metode henon map ini, jika salah satu nilai parameter menggunakan nilai yang berbeda dari 1,4 dan 0,3 maka akan diperoleh nilai yang akan mengarah ke satu hasil yang sama untuk tiap iterasinya.

2.2 Pengumpulan Data

Data pada penelitian menggunakan sekunder yang didapat dari internet dan jurnal lain, data citra yang digunakan dapat dilihat pada gambar 2.

(a) (b) (d) (e)

Gambar 2. Data citra

2.3 Perancangan Algoritma Kriptografi

Pada tahapan perancangan algoritma kriptografi dijelaskan bagaimana proses enkripsi dan dekripsi menggunakan perpaduan *Logistic map* dan *Henon Map.*

a. Enkripsi
Enkripsi citra dilakukan dengan cara melakukan perubahan terhadap nilai bit piksel pada citra digital, terdapat dua tahapan enkripsi dalam penelitian ini, tahap awal enkripsi citra adalah melakukan pengacakan bit pixel menggunakan Logistic Map dan dilanjutkan dengan melakukan xor tiap bit piksel secara acak menggunakan Henon Map, Langkah – Langkah enkripsi akan dijelaskan adalah sebagai berikut:
Langkah – Langkah enkripsi tahap 1:
1. Pada tahapan awal, diperlukannya ekstraksi bit RGB, citra akan diubah menjadi array list yang terdiri dari nilai bit RGB, contoh hasil ekstraksi sebagai berikut dengan asumsi Panjang array adalah 20.
[255, 123, 132, 56, 90, 12, 45, 64, 112, …]
2. Setelah proses ekstraksi dilakukan akan dilanjutkan dengan proses pengacakan bit piksel, pengacakan dilakukan secara continue dimulai dari index 0 sampai dengan index n, pada tahap ini digunakan perhitungan Logistic Map sebagai penentu tujuan index yang akan ditukar. Contoh:
Index yang akan ditukar adalah index 0, kunci user (x) adalah 0.1 dan *r* sama dengan 3,9, maka diperoleh perhitungan Logistic Map sebagai berikut:
$x_{n+1} = r x_n (1 - x_n)$
$x_2 = 3{,}95\ 0{,}12_1 (1 - 0{,}12_1)$
$x_2 = 0{,}41712$
Setelah nilai x_2 diperoleh akan dilanjutkan dengan mengubah nilai tersebut menjadi nilai desimal dengan melakukan perkalian x_2 dengan 10^{16} dan mod panjang array.
$x_2 = 0{,}41712 \times 10^{16} \,\%\, 20$
$x_2 = 12$
Hasil perhitungan mendapatkan nilai 12, sehingga index 0 pada array akan ditukar dengan index 12, dan kedua index tersebut akan diberi penanda agar tidak ditukar lagi pada iterasi selanjutnya, enkripsi tahap 1 selesai sampai pada tahap ini dan akan akan dilanjutkan ke enkripsi tahap 2 menggunakan *Henon Map.*

Langkah – Langkah enkripsi tahap 2:
1. Array nilai piksel RGB yang telah di acak pada tahap 1 akan dixor dengan nilai hasil dari perhitungan *Henon Map.*
2. Pada tahap ini akan digunakan dua kunci yang didapatkan dari perhitungan *Logistic Map* dan kunci yang dimasukan oleh user.
Contoh perhitungan *Henon Map* sebagai berikut ini.
Kunci yang dimasukan user (x) adalah 0.1, kunci yang dibuat oleh sistem (y) adalah 0.003, a = 1.4 dan b = 0.3.
$x_{n+1} = 1 - a\ x_1^2 + y_1$
$x_2 = 1 - 1{,}4\ 0{,}1^2 + 0{,}3$
$x_2 = 0{,}989$

$y_{n+1} = b\ x_n$
$y_2 = 0.3\ 0.1$
$y_2 = 0.03$
Setelah nilai kedua proses perhitungan diperoleh akan dilanjutkan dengan mengubah nilai tersebut menjadi nilai desimal dengan melakukan perkalian dengan 10^{16} dan nilai x akan di mod dengan Panjang array dan nilai y akan di mod dengan nilai maksimal piksel (255).
$x = 0{,}989 \times 10^{16} \,\%\, 20$
$x = 9$
$y = 0{,}03 \times 10^{16} \,\%\, 255$
$y = 3$
Setelah proses mod selesai, nilai x akan digunakan sebagai penunjuk nilai yang akan dilakukan proses xor dan nilai y akan di xor dengan nilai yang ada pada index 9 sesuai dengan nilai x.
3. Proses terakhir adalah melakukan pembentukan citra dari array list.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

b. Dekripsi
Pada tahap dekripsi terdapat sedikit perbedaan dari proses enkripsi, proses dekripsi diawali dengan proses xor dan di lanjutnkan dengan proses pengembalian acakan. Langkah – Langkah dekripsi sebagai berikut.
Langkah – Langkah dekripsi tahap 1:
1. Langkah awal dekripsi adalah mengubah citra menjadi array menjadi array list RGB.
2. Dilanjutkan dengan melakukan xor dengan perhitungan *Henon Map*

Langkah – Langkah enkripsi tahap 2:
1. Setelah xor selesai akan dilakukan proses mengembalikan acakan dengan perhitungan logistic map.
2. Begitu proses selesai akan dilakukan pembelikan Kembali citra berdasarkan list array.

2.4 Implementasi sistem

Proses implementasi *Logistic Map* dan *Henon Map* ini akan dilakukan menggunakan bahasa pemrograman python dengan interpreter pycharm, proses pengacakan menggunakan *Logistic Map* dapat dilihat pada kode berikut ini.

```
def enkripsi_1(key1, key2, size, pixel):
    r = 3.95
    count = 0
    x = key1
    flat_pixel = pixel.ravel()
    array_bantu = []
    for i in range(size):
        array_bantu.append(-1)
    while count in range(size):
        x = r * x * (1 - x) # logistik Map
        temp = int((x * pow(10, 16)) % size)
        if array_bantu[temp] == -1:
            array_bantu[temp] = flat_pixel[count]
        else:
            count -= 1
        count += 1
    cipher_pixel = np.array(list(enkripsi_2(key1, key2, size,
array_bantu)))
    cipher_pixel = cipher_pixel.reshape((int(size/4), 4))
    return cipher_pixel
```

Nilai hasil perhitungan logistic map berupa float yang kurang dari 1 oleh karena itu perlu dilakukan proses untuk melakukan perubahan pada nilai float tersebut menjadi nilai desimal yang dapat digunakan sebagai penunjuk index pertukaran, setelah seluruh bit piksel ditukar proses akan dilanjutkan ke proses enkripsi tahap dua, tahap enkripsi ini menggunakan teori *Henon Map* dalam menentukan nilai citra yang akan digunakan dalam proses XOR dan juga index yang akan di XOR.

```
def enkripsi_2(key1, key2, size, pixel):
    x = key1
    y = key2
    kontrol = []
    array_bantu = []
    count = 0
    for i in range(size):
        array_bantu.append(-1)
    while count in range(size):
        x1 = 1 - 1.4 * x * x + y #henon map
        y1 = 0.3 * x             #henon map
        x = x1
        y = y1
        k1 = int((x1 * pow(10, 16)) % size)
        k2 = int((y1 * pow(10, 16)) % 256)
        if array_bantu[k1] == -1:
```

```
            array_bantu[k1] = k2
        else:
            count -= 1
        kontrol.append(k1)
        count += 1
    for i in range(size):
        pixel[i] = pixel[i] ^ array_bantu[i]
    return pixel
```

Pada enkripsi tahap dua ini dilakukan XOR bit piksel gambar, pada tahap ini digunakan teori *Henon Map*, teori ini menghasilkan dua nilai, source kode diatas menunjukan hasil perhitungan pertama (x) akan dijadikan penunjuk index yang ingin di XOR sedangkan nilai kedua (y) akan dijadikan nilai bit baru untuk proses XOR. proses ini digunakan dua list baru untuk membantu perhitungan XOR hal ini digunakan karena proses XOR akan dilakukan pada bit piksel acak sesuai dengan nilai k1, nilai k1 merupakan nilai x yang telah diproses menjadi nilai desimal, sedangkan nilai dari k2 akan digunakan sebagai nilai yang akan di XOR dengan nilai bit piksel, enkripsi di akhiri dengan melakukan *save image*.

2.5 Pengujian sistem.

Tujuan pengujian dilakukan untuk menguji kelayakan sistem dan mengecek kembali apabila terdapat kesalahan pada sisrem maka sistem akan diperbaiki. Pada penelitian ini dilakukan pengujian PSNR dan MSE.

Peak Signal to Noise Ratio (PSNR) adalah metode untuk melakukan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR dinyatakan dalam satuan decibel (dB). Dalam proses mendapatkan nilai PSNR diperlukan nilai MSE (Mean Square Error) terlebih dahulu. MSE adalah nilai error kuadrat rata-rata antara citra asli (*plain image*) dengan citra manipulasi (*cipher image*), Berikut merupakan rumus persamaan MSE dan PSNR. Berikut ini adalah persamaan yang digunakan dalam menentukan nilai MSE dan PSNR.

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{M} \left(C_{xy} - P_{xy}\right)^2 \quad (4)$$

Keterangan :

$M \; dan \; N$: Dimensi citra yang akan diperoses

C_{xy} : Nilai piksel *cipher image* pada koordinat x dan y

P_{xy} : Nilai piksel *plain image* pada koordinat x dan y

$$PSNR = 20 \log 10 \left(\frac{\max\_pixel}{MSE}\right) \quad (5)$$

Keterangan :

$\max\_pixel$: Nilai maksimum piksel pada citra

Nilai MSE yang diperoleh pada persamaan (4) digunakan pada persamaan (5) sebagai pembagi nilai pixel maksimum pada citra asli. Nilai PSNR inilah yang menjadi pedoman apakah sebuah citra memiliki kualitas yang baik atau tidak. Nilai yang dihasilkan oleh PSNR dapat mencapai nilai tak hingga yang diakibatkan oleh nilai MSE yang sama dengan 0, oleh sebab itu nilai PSNR dibatasi hanya sampai dengan 100dB.

Nilai PSNR dibawah 30 dB mengindikasikan kualitas yang relatif rendah, dimana distorsi yang disebabkan oleh perlakuan terlihat dengan jelas [10]. Pengujian PSNR dan MSE ini dilakukan untuk mengetahui kemampuan enkripsi perpaduan *Logistic Map* dan *Henon Map* pengujian ini akan dilakukan dengan membandingkan citra asli dengan citra hasil enkripsi, pengujian diawali dengan melakukan enkripsi citra dengan kunci yang sama, setelah proses enkripsi selesai proses akan dilanjutkan dengan melakukan proses penghitungan nilai PSNR dan MSE.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

2.6 Analisis

Pada tahapan analisis akan dibandingkan nilai MSE dan PSNR yang di dapatkan oleh citra digital yang telah di enkripsi proses ini akan dilakukan dengan mengikuti pedoman nilai pada tabel berikut ini.

Tabel 1. Tingkat Nilai MSE

Nilai MSE	Akurasi eror
< 40	Sangat baik
41 sampai 100	Cukup baik
101 sampai 200	Baik
201 sampai 300	Sangat buruk
> 400	Buruk

Tabel 2. Tingkat Nilai PSNR

Nilai PSNR (dB)	Kualitas Sinyal
> 30	Sangat baik
25 sampai 30	Baik
20 sampai 24	Cukup buruk
11 sampai 19	Buruk
< 10	Sangat buruk

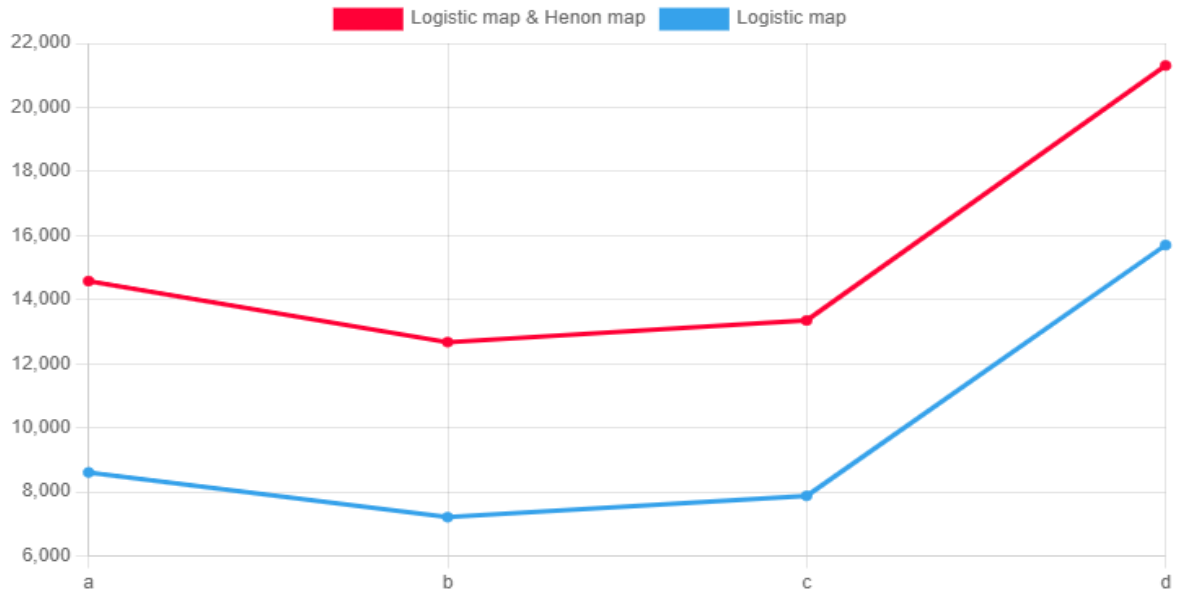
3. Result and Discussion

Pada bagian ini akan di tampilkan hasil dari pengujian program yang meliputi, nilai kualitas citra berdasarkan MSE dan PSNR, nilai MSE dan PSNR dari pada penelitian ini akan dibandingkan dengan nilai MSE dan PSNR dari metode enkripsi menggunakan *Logistic Map,* selain perbandingan nilai MSE dan PSNR akan dilakukan analisis perubahan citra asli dan citra yang telah melalui proses kriptografi. Hasil enkripsi citra dapat dilihat pada gambar 3.

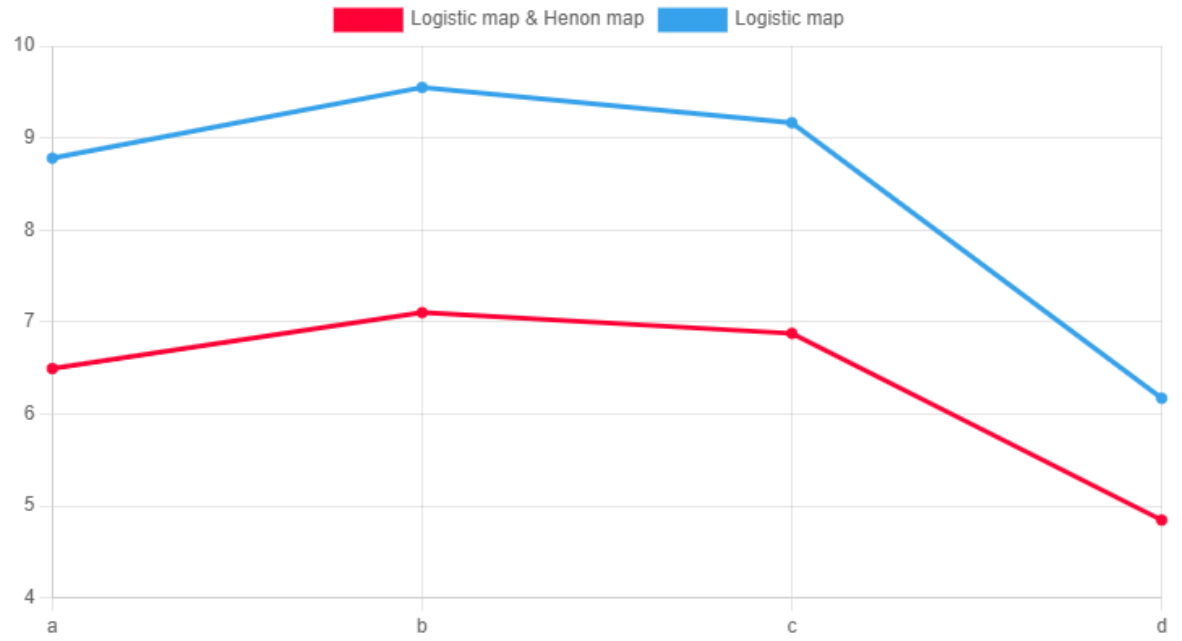
Gambar 3. (f) adalah hasil enkripsi (a), (b) adalah hasil enkripsi (g), (d) adalah hasil enkripsi (h), (e) adalah hasil enkripsi (i).

3.1. Uji MSE dan PSNR

Tahap ini adalah tahap membandingkan *cipher image* yang yang di enkripsi dengan *Logistic Map* dan pada *cipher image* yang dihasilkan dari perpaduan *Logistic Map* dan *Henon Map,* perbandingan nilai MSE dapat dilihat pada gambar 4 dan perbandingan nilai PSNR dapat dilihat pada gambar 5.



Gambar 4. Grafik MSE *Cipher image vs Plain image*



Gambar 5. Grafik PSNR *Cipher image vs Plain image*

diketahui bahwa terdapat peningkatan keamanan citra digital yang di enkripsi menggunakan perpaduan Logistic Map dan Henon Map yang dibandingkan dengan citra yang hanya di enkripsi dengan menggunakan Logistic Map. Peningkatan tersebut dibuktikan dengan rata – rata nilai MSE yang diperoleh oleh citra yang di enkripsi menggunakan perpaduan Logistic map dan Henon Map lebih besar dari rata – rata nilai MSE yang diperoleh oleh citra yang di enkripsi dengan Logistic Map saja. Sebaliknya dengan PSNR makin kecil nilai PSNR maka semakin besar banyak *noise*.

3.2. Analisis Luaran

Dalam pengujian metode ini diperlukan analisis lanjutan untuk mengetahui pengaruh dari enkripsi dan dekripsi terhadap *plain image*, informasi mengenai citra dapat dilihat pada tabel 3. pada tabel 3 terdapat informasi basar file, dimensi citra, dan waktu yang dibutuhkan dalam melakukan enkripsi.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Tabel 3. Inforrmasi citra

No	Citra enkripsi	Waktu (*seconds*)	Dimensi	Besar file (KB)		
				Plain image	*Cipher image*	*Decrypted image*
1	a	39.0	500 × 500	132	978	120
2	b	49.13	512 × 512	459	1024	422
3	c	18.30	429 × 285	239	478	222
4	d	22.92	460 × 333	25,8	599	26,2

Pada tabel 3 dapat diketahui bahwa terdapat perbedaan ukuran file diantara *plain image* dengan *cipher image* dan *plain image* dengan *decrypted image*, *cipher image* memiliki ukuran file yang lebih besar dari *plain image* namun sebaliknya untuk *decrypted image*, ukuran file yang dimiliki *decrypted image* lebih kecil dari ukuran file yang dimiliki oleh *plain image*, namun perubahan ukuran file tidak mempengaruhi kualitas citra dan ukuran dimensi citra. Selain mengetahui terdapat perbedaan ukuran file yang dihasilkan dapat dilihat juga semakin besar ukuran dimensi citra akan mempengaruhi waktu proses enkripsi dan dekripsi citra digital, untuk pembahasan lebih lanjut dilakukan pengujian pengaruh ukuran citra pada

4. Kesimpulan

Kesimpulan yang dapat ditarik dari penelitian ini adalah, sistem enkripsi yang memadukan *Logistic Map* dan *Henon Map* menghasilkan nilai PSNR rata - rata kurang dari 10 dB yang mengindikasikan bahwa citra hasil enkripsi memiliki *noise* yang sangat tinggi dan nilai MSE yang lebih dari 400, hal ini mengartikanya banyaknya eror sinyal dari citra asli dan cipher image. Lamanya proses yang diperlukan untuk melakukan proses enkripsi dan dekripsi sangat dipengaruhi oleh besarnya dimensi dan banyaknya piksel yang ada pada suatu citra digital, sistem enkripsi menggunakan perpaduan Logistic Map dan Henon Map ini memerlukan waktu lebih dari 15 detik dalam melakukan enkripsi citra yang memiliki ukuran dimensi 512×512, namun hasil enkripsi citra tidak terpengaruh oleh ukuran dimensi citra yang di enkripsi

References

[1] V. A. Manoppo, A. S. M. Lumenta, and S. D. S. Karouw, “Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi,” *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.

[2] R. A. Nugraha, “Sistem Steganography Dengan Metode Least Signifcant Bit (Lsb) & Metode Caesar Cipher Berbasis Android,” *Skripsi*, 2019, doi: 10.30873/ji.v20i1.1615.

[3] D. Pradeka, “PENYEMBUNYIAN INFORMASI DENGAN METODE CRYPTO-STEGANOGRAPHY MENGGUNAKAN MEDIA GAMBAR BERBASIS MOBILE,” *Pros. Semin. Nas. 2018*, 2018.

[4] H. Gao, Y. Zhang, S. Liang, and D. Li, “A new chaotic algorithm for image encryption,” *Chaos, Solitons and Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[5] A. Susanto, “Penerapan Teori Chaos di dalam Kriptografi,” *J. Tek. Inform.*, 2008.

[6] R. Munir, “Algoritma Enkripsi Citra Digital Dengan Kombinasi Dua Chaos,” Yogyakarta: 15-16 Juni, 2019.

[7] M. Babaei, “A novel text and image encryption method based on chaos theory and DNA computing,” *Nat. Comput.*, vol. 12, no. 1, pp. 101–107, 2013, doi: 10.1007/s11047-012-9334-9.

[8] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, “A new algorithm for digital image encryption based on chaos theory,” *Entropy*, vol. 23, no. 3, pp. 1–16, 2021, doi: 10.3390/e23030341.

[9] P. Ping, F. Xu, Y. Mao, and Z. Wang, “Designing permutation–substitution image encryption networks with Henon map,” *Neurocomputing*, vol. 283, pp. 53–63, 2018, doi: 10.1016/j.neucom.2017.12.048.

[10] H. Sajati, “ANALISIS KUALITAS PERBAIKAN CITRA MENGGUNAKAN METODE MEDIAN FILTER DENGAN PENYELEKSIAN NILAI PIXEL,” *J. Ilm. Bid. Teknol.*, vol. x, no. 1, pp. 41–48, 2018.

This page is intentionally left blank.