

Implementasi Pembangkit Bilangan Acak Semu dengan Tinkerbell-Hénon Hyperchaotic Map

Dzaky Satrio Nugroho - 13522059^{1,2}

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

¹13522059@stei.itb.ac.id, ²dzakysatrio0122@gmail.com

Abstrak—Kriptografi merupakan bidang ilmu yang terus berkembang untuk menjamin kerahasiaan, integritas, dan autentikasi data, yang sangat bergantung pada kualitas bilangan acak. Salah satu pendekatan yang banyak diteliti dalam perancangan pembangkit bilangan acak semu adalah pemanfaatan teori chaos, karena sifatnya yang sensitif terhadap kondisi awal dan bersifat tidak terprediksi. Makalah ini berfokus pada dua sistem chaos dua dimensi, yaitu Tinkerbell map dan Hénon map, yang masing-masing memiliki karakteristik dinamika nirlanjar yang kompleks. Berdasarkan penggabungan dinamika kedua map tersebut, diusulkan suatu skema pembangkit bilangan acak semu baru berbasis Tinkerbell-Hénon hyperchaotic map yang diharapkan memiliki kompleksitas dan tingkat keamanan yang lebih tinggi dibandingkan penggunaan satu map secara tunggal. Makalah ini memaparkan proses perancangan dan implementasi pembangkit bilangan acak semu tersebut, serta melakukan analisis kualitas keacakannya menggunakan beberapa metrik statistik dan karakteristik chaos untuk mengevaluasi performa dan kelayakannya dalam aplikasi kriptografi.

Keywords—Hénon Map, Pembangkit Bilangan Acak, Teori Chaos, Tinkerbell Map.

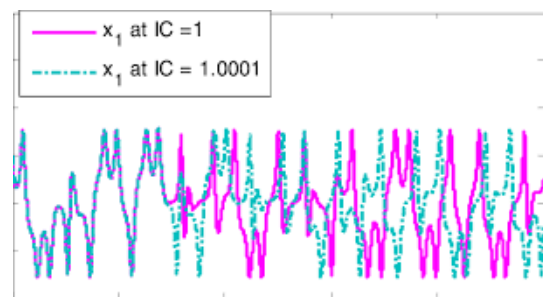
I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat mendorong meningkatnya kebutuhan akan sistem keamanan data yang andal. Kriptografi berperan penting dalam menjaga kerahasiaan, integritas, serta autentikasi informasi, baik dalam komunikasi digital, penyimpanan data, maupun sistem terdistribusi. Salah satu komponen fundamental dalam kriptografi adalah bilangan acak, yang digunakan dalam berbagai mekanisme seperti pembangkitan kunci, *nonce*, *initialization vector*, dan protokol keamanan lainnya.

Dalam praktiknya, bilangan acak yang digunakan pada sistem komputasi umumnya dihasilkan oleh pembangkit bilangan acak semu (*pseudorandom number generator*). Pembangkit ini bersifat deterministik dan bergantung pada nilai awal tertentu, namun harus mampu menghasilkan urutan bilangan yang sulit diprediksi dan memiliki sifat statistik yang menyerupai bilangan acak sejati. Kelemahan pada pembangkit bilangan acak semu dapat berdampak serius terhadap keamanan sistem kriptografi, sehingga diperlukan metode pembangkitan

yang memiliki tingkat keacakan dan kompleksitas yang tinggi.

Salah satu pendekatan yang banyak dikembangkan dalam penelitian pembangkit bilangan acak semu adalah pemanfaatan teori chaos. Sistem chaos memiliki sifat deterministik namun sangat sensitif terhadap kondisi awal, sehingga perubahan kecil pada parameter atau nilai awal dapat menghasilkan perbedaan keluaran yang signifikan. Karakteristik ini membuat sistem chaos tampak acak dan sulit diprediksi, sehingga cocok untuk diaplikasikan dalam bidang kriptografi dan keamanan informasi.



Gambar 1. Sensitivitas kondisi awal (Borah dkk., 2016)

Beberapa peta chaos diskrit dua dimensi, seperti Hénon map dan Tinkerbell map, telah banyak diteliti dan digunakan sebagai dasar pembangkit bilangan acak semu. Hénon map dikenal dengan struktur sederhana namun memiliki atraktor fraktal yang kompleks, sedangkan Tinkerbell map menawarkan dinamika nirlanjar yang lebih kaya dengan ruang parameter yang lebih luas. Penggabungan dua sistem chaos ini berpotensi menghasilkan sistem hyperchaotic yang memiliki lebih dari satu eksponen Lyapunov positif, sehingga meningkatkan kompleksitas dinamika dan kualitas keacakan yang dihasilkan.

Berdasarkan latar belakang tersebut, penelitian ini mengusulkan implementasi pembangkit bilangan acak semu berbasis Tinkerbell-Hénon hyperchaotic map. Fokus utama penelitian ini adalah merancang dan mengimplementasikan model pembangkit bilangan acak semu yang memanfaatkan penggabungan kedua peta chaos tersebut, serta menganalisis kualitas bilangan acak yang dihasilkan menggunakan beberapa metrik dan uji

statistik. Diharapkan hasil penelitian ini dapat memberikan kontribusi dalam pengembangan pembangkit bilangan acak semu yang lebih aman dan andal untuk aplikasi kriptografi.

II. TEORI DASAR

A. Bilangan Acak Semu

Bilangan acak semu (*pseudorandom*) merupakan deretan bilangan yang dihasilkan oleh suatu algoritma deterministik, namun memiliki karakteristik statistik yang menyerupai bilangan acak sejati. Berbeda dengan bilangan acak sejati yang bersumber dari fenomena fisik yang tidak dapat diprediksi, bilangan acak semu dihasilkan menggunakan nilai awal tertentu yang disebut *seed*. Dengan *seed* yang sama, algoritma pembangkit bilangan acak semu akan menghasilkan urutan bilangan yang identik, sehingga proses ini bersifat dapat direproduksi.

Dalam bidang kriptografi, bilangan acak semu memegang peranan yang sangat penting, khususnya dalam pembangkitan kunci, inisialisasi vektor, nonce, serta berbagai mekanisme keamanan lainnya. Kualitas bilangan acak semu yang digunakan secara langsung memengaruhi tingkat keamanan suatu sistem kriptografi. Oleh karena itu, pembangkit bilangan acak semu harus memenuhi beberapa sifat utama, seperti distribusi yang uniform, periode yang panjang, serta tingkat ketidakterkaitan yang tinggi antar bilangan yang dihasilkan.

Suatu pembangkit bilangan acak semu yang baik juga harus memiliki tingkat *unpredictability* yang tinggi, sehingga sulit bagi pihak yang tidak berwenang untuk menebak nilai berikutnya meskipun sebagian urutan bilangan telah diketahui. Kelemahan pada pembangkit bilangan acak semu dapat dimanfaatkan untuk melakukan serangan kriptografi, seperti *key recovery* atau *state prediction*.

B. Teori Chaos

Teori chaos merupakan cabang dari matematika yang mempelajari perilaku sistem dinamik nirlanjar yang sangat sensitif terhadap kondisi awal. Sistem chaos bersifat deterministik, namun evolusi keadaannya sulit diprediksi dalam jangka panjang karena perbedaan kecil pada kondisi awal dapat menghasilkan perbedaan keluaran yang sangat besar. Sifat ini dikenal sebagai *sensitive dependence on initial conditions* dan sering diasosiasikan dengan istilah *butterfly effect*.

Sistem chaos umumnya memiliki beberapa karakteristik utama, antara lain sensitivitas terhadap kondisi awal, topologi yang bercampur, serta orbit periodik yang rapat. Karakteristik tersebut menyebabkan keluaran sistem chaos tampak acak meskipun dibangkitkan melalui persamaan matematis yang deterministik. Contoh sistem chaos yang banyak diteliti antara lain Logistic map, Hénon map, Tinkerbell map, dan berbagai peta chaos diskrit dua dimensi lainnya.

Dalam konteks kriptografi dan pembangkit bilangan

acak semu, teori chaos dimanfaatkan karena kemampuannya menghasilkan urutan bilangan dengan kompleksitas tinggi dan tingkat *unpredictability* yang baik. Sistem chaos diskrit sangat sesuai untuk implementasi digital karena memiliki bentuk persamaan yang sederhana dan efisien secara komputasi. Dengan pemilihan parameter dan kondisi awal yang tepat, sistem chaos dapat menghasilkan urutan bilangan dengan distribusi yang mendekati uniform dan korelasi yang rendah.

Pengembangan lebih lanjut dari sistem chaos menghasilkan konsep hyperchaos, yaitu sistem yang memiliki lebih dari satu eksponen Lyapunov positif. Keberadaan lebih dari satu eksponen Lyapunov positif menunjukkan tingkat kompleksitas dinamika yang lebih tinggi dibandingkan sistem chaos biasa. Dalam penelitian ini, konsep hyperchaos dimanfaatkan melalui penggabungan dua peta chaos, yaitu Tinkerbell map dan Hénon map, untuk meningkatkan kualitas keacakan dan keamanan pembangkit bilangan acak semu yang dihasilkan.

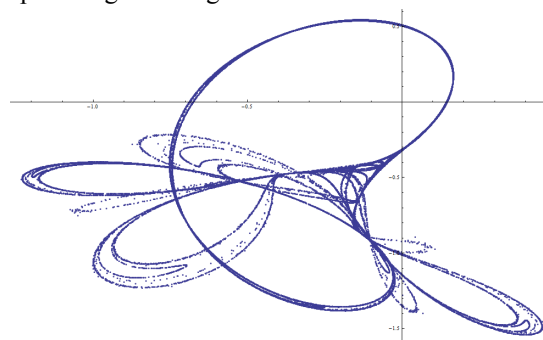
C. Tinkerbell Map

Tinkerbell map merupakan sistem dinamik diskrit dua dimensi yang juga menunjukkan perilaku chaos untuk nilai parameter tertentu. Tinkerbell map didefinisikan oleh persamaan sebagai berikut:

$$\begin{aligned}x_{n+1} &= x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} &= 2x_n y_n + cx_n + dy_n\end{aligned}$$

dengan a , b , c , dan d merupakan parameter sistem, serta x_n dan y_n menyatakan keadaan sistem pada iterasi ke- n . Sistem ini dikenal memiliki dinamika yang kompleks dan atraktor chaos yang kaya, bergantung pada kombinasi parameter yang digunakan.

Dibandingkan dengan Hénon map, Tinkerbell map memiliki tingkat nirlanjar yang lebih tinggi karena melibatkan lebih banyak parameter dan interaksi silang antara variabel. Hal ini menghasilkan ruang kunci yang lebih luas apabila diterapkan dalam sistem kriptografi. Sensitivitas tinggi terhadap perubahan kecil pada parameter maupun kondisi awal menjadikan Tinkerbell map sulit diprediksi dan sesuai untuk digunakan sebagai dasar pembangkit bilangan acak semu.



Gambar 2. *Tinkerbell attractor* untuk $a = 0,9$, $b = -0,613$, $c = 2$, dan $d = 0,5$

Dalam aplikasi pembangkit bilangan acak semu berbasis chaos, Tinkerbell map sering digunakan untuk

meningkatkan kompleksitas dan memperpanjang periode bilangan acak yang dihasilkan. Kombinasi Tinkerbell map dengan peta chaos lainnya, seperti Hénon map, dapat menghasilkan sistem hyperchaotic yang memiliki tingkat keacakan dan keamanan yang lebih tinggi, sehingga lebih robust terhadap serangan analisis statistik maupun prediksi.

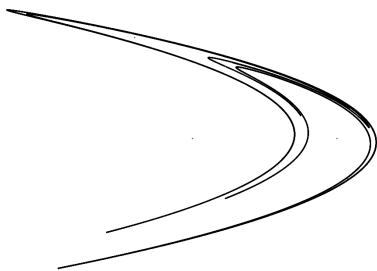
D. Hénon Map

Hénon map merupakan salah satu sistem dinamik diskrit dua dimensi yang diperkenalkan oleh Michel Hénon sebagai penyederhanaan dari sistem Lorenz. Hénon map didefinisikan oleh pasangan persamaan nirlanjar sebagai berikut:

$$\begin{aligned}x_{n+1} &= 1 - ax_n^2 + y_n \\ y_{n+1} &= bx_n\end{aligned}$$

dengan a dan b merupakan parameter sistem, sedangkan x_n dan y_n menyatakan keadaan sistem pada iterasi ke- n . Untuk nilai parameter tertentu, seperti $a = 1,4$ dan $b = 0,3$, Hénon map menunjukkan perilaku chaos yang kuat dengan atraktor fraktal yang kompleks.

Karakteristik utama Hénon map adalah sensitivitas yang tinggi terhadap kondisi awal serta dinamika nirlanjar yang menghasilkan lintasan yang tampak acak. Sifat-sifat tersebut menjadikan Hénon map banyak dimanfaatkan dalam berbagai aplikasi, termasuk kriptografi, pengacakan citra, dan pembangkit bilangan acak semu. Selain itu, struktur dua dimensinya memungkinkan peningkatan kompleksitas dibandingkan peta chaos satu dimensi, sehingga lebih sulit untuk dianalisis atau diprediksi oleh pihak yang tidak berwenang.



Gambar 3. Hénon attractor untuk $a = 1,4$ dan $b = 0,3$

Dalam pembangkit bilangan acak semu, keluaran Hénon map dapat dimanfaatkan dengan melakukan normalisasi atau transformasi tertentu agar sesuai dengan rentang bilangan yang diinginkan. Pemilihan parameter dan kondisi awal yang tepat sangat berpengaruh terhadap kualitas keacakan yang dihasilkan, karena nilai parameter di luar daerah chaos dapat menyebabkan sistem bersifat periodik atau konvergen.

III. IMPLEMENTASI

Pembangkit bilangan acak yang dihasilkan dari gabungan Tinkerbell map dan Hénon map adalah sebagai berikut :

Formula matematika di atas diimplementasikan dengan program python untuk membangkitkan bilangan acak. Berikut merupakan potongan program yang memanfaatkan fungsi di atas:

```
def henon_map(x0, y0, a=1.4, b=0.3, n=10000,
discard=1000):
```

```
    x, y = x0, y0
    xs, ys = [], []
```

```
    for i in range(n):
        x_next = 1 - a * x**2 + y
        y_next = b * x
        x, y = x_next, y_next
```

```
    if i > discard:
        xs.append(x)
        ys.append(y)
```

```
    return np.array(xs), np.array(ys)
```

```
x, y = henon_map(0.1, 0.1)
```

```
plt.figure()
plt.scatter(x, y, s=0.1)
plt.title("Phase Diagram - Henon Map")
plt.xlabel("x")
plt.ylabel("y")
plt.show()
```

```
a_values = np.linspace(1.0, 1.5, 400)
x0, y0 = 0.1, 0.1
```

```
A, X = [], []
```

```
for a in a_values:
    x, y = x0, y0
    for i in range(2000):
        x = 1 - a * x**2 + y
        y = 0.3 * x
    if i > 1500:
        A.append(a)
        X.append(x)
```

```
plt.figure()
plt.scatter(A, X, s=0.1)
plt.title("Bifurcation Diagram - Henon Map (parameter a)")
plt.xlabel("a")
plt.ylabel("x")
plt.show()
```

```
def tinkerbell_map(x0, y0, a=0.9, b=-0.6013, c=2.0,
d=0.5, n=10000, discard=1000):
    x, y = x0, y0
```

```

xs, ys = [], []

for i in range(n):
    x_next = x**2 - y**2 + a*x + b*y
    y_next = 2*x*y + c*x + d*y
    x, y = x_next, y_next

    if i > discard:
        xs.append(x)
        ys.append(y)

return np.array(xs), np.array(ys)

x, y = tinkerbell_map(0.1, 0.1)

plt.figure()
plt.scatter(x, y, s=0.1)
plt.title("Phase Diagram - Tinkerbell Map")
plt.xlabel("x")
plt.ylabel("y")
plt.show()

a_values = np.linspace(0.85, 0.95, 500)
x0, y0 = 0.1, 0.1

A, X = [], []

for a in a_values:
    x, y = x0, y0

    for i in range(3000):
        x_new = x**2 - y**2 + a*x - 0.6013*y
        y_new = 2*x*y + 2.0*x + 0.5*y

        # CLIPPING to avoid overflow
        if abs(x_new) > 10 or abs(y_new) > 10:
            break

    x, y = x_new, y_new

    # Ambil steady-state
    if i > 2500:
        A.append(a)
        X.append(x)

plt.figure(figsize=(8,5))
plt.scatter(A, X, s=0.1)
plt.title("Bifurcation Diagram - Tinkerbell Map (parameter a)")
plt.xlabel("a")
plt.ylabel("x")
plt.show()

def hybrid_map(x0, y0, u0, v0, n=10000, discard=1000):
    # Parameters
    a, b, c, d = 0.9, -0.6013, 2.0, 0.5
    alpha, beta = 1.4, 0.3

    x, y = x0, y0

```

```

u, v = u0, v0

zx, zy = [], []

for i in range(n):
    # Tinkerbell
    x_next = x**2 - y**2 + a*x + b*y
    y_next = 2*x*y + c*x + d*y

    # Henon
    u_next = 1 - alpha * u**2 + v
    v_next = beta * u

    x, y = x_next, y_next
    u, v = u_next, v_next

    # Mixing
    z1 = x + u
    z2 = y + v

    if i > discard:
        zx.append(z1)
        zy.append(z2)

return np.array(zx), np.array(zy)

z1, z2 = hybrid_map(0.1, 0.1, 0.2, 0.2)

plt.figure()
plt.scatter(z1, z2, s=0.1)
plt.title("Phase Diagram - Hybrid Tinkerbell-Henon Map")
plt.xlabel("z1")
plt.ylabel("z2")
plt.show()

alpha_values = np.linspace(1.2, 1.45, 500)

x0, y0 = 0.1, 0.1
u0, v0 = 0.1, 0.1

A, Z = [], []

for alpha in alpha_values:
    x, y = x0, y0
    u, v = u0, v0

    for i in range(3000):
        # Tinkerbell
        x_new = x**2 - y**2 + 0.9*x - 0.6013*y
        y_new = 2*x*y + 2.0*x + 0.5*y

        # Henon
        u_new = 1 - alpha * u**2 + v
        v_new = 0.3 * u

        # CLIPPING
        if max(abs(x_new), abs(y_new), abs(u_new), abs(v_new)) > 10:
            break

```

```

x, y = x_new, y_new
u, v = u_new, v_new

z = x + u

if i > 2500:
    A.append(alpha)
    Z.append(z)

plt.figure(figsize=(8,5))
plt.scatter(A, Z, s=0.1)
plt.title("Bifurcation Diagram - Hybrid
Tinkerbell-Henon Map (parameter  $\alpha$ )")
plt.xlabel(" $\alpha$ ")
plt.ylabel("z")
plt.show()

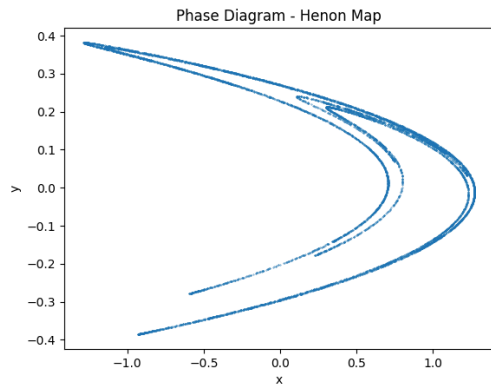
```

IV. HASIL DAN ANALISIS

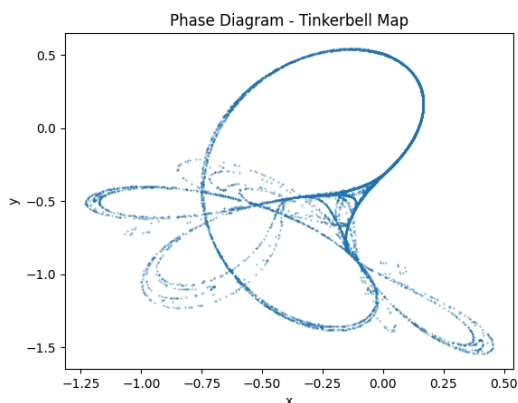
Tinkerbell-Henon map yang diusulkan memiliki behavior chaos yang lebih baik dibandingkan dengan dua map awal. Berikut merupakan hasil analisis chaotic map yang telah dibuat.

A. Phase Diagram

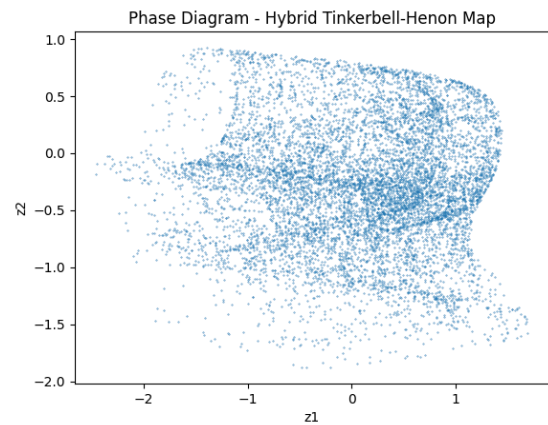
Pada pembangkitan bilangan acak, *phase diagram* digunakan untuk memvisualisasikan hubungan antara nilai x_n dengan nilai x_{n+1} .



Gambar 4. Phase Diagram Hénon Map



Gambar 5. Phase Diagram Tinkerbell Map

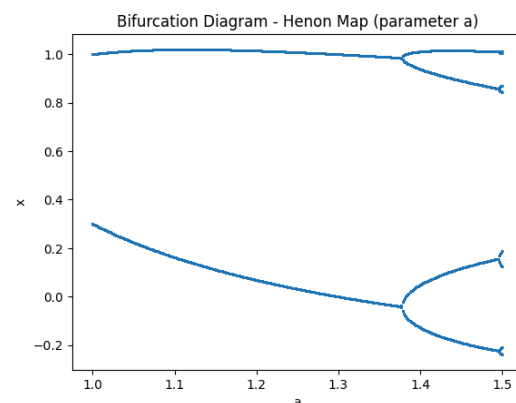


Gambar 6. Phase Diagram Tinkerbell-Hénon Map

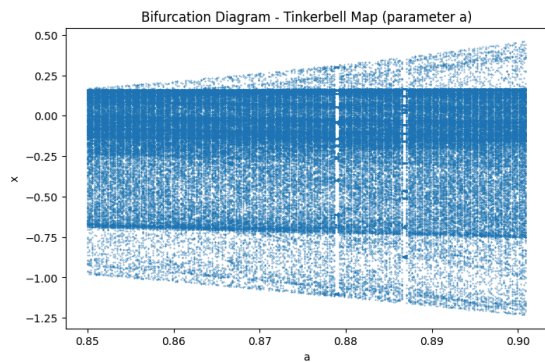
Dengan menetapkan nilai awal dan parameter yang identik pada ketiga fungsi tersebut, dapat diamati bahwa *Tinkerbell-Hénon Map* memiliki sebaran fase yang mencakup hampir seluruh area bidang dan menunjukkan distribusi yang lebih merata dibandingkan dengan diagram fase Hénon Map maupun Tinkerbell Map. Seperti ditunjukkan pada Gambar 4 dan Gambar 5, lintasan yang dihasilkan oleh Hénon Map dan Tinkerbell Map relatif sederhana serta cenderung menunjukkan perilaku deterministik. Kondisi ini menyebabkan kedua map tersebut lebih mudah diprediksi dan kurang memadai dari sisi keamanan. Sebaliknya, Hénon-Sine Map memiliki tingkat ergodisitas yang lebih tinggi sehingga mampu menghasilkan keluaran dengan tingkat keacakan yang lebih baik dibandingkan dengan Henon Map dan Sine Map.

B. Bifurcation Diagram

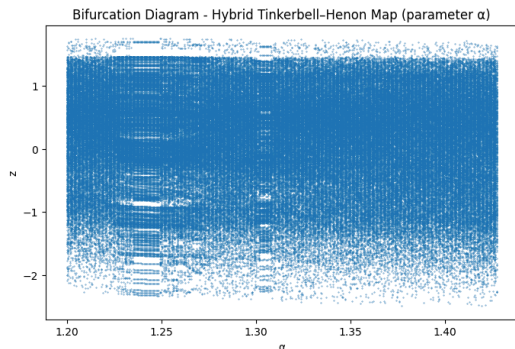
Bifurcation Diagram merupakan representasi visual yang digunakan untuk menunjukkan perubahan dinamika suatu sistem nonlinier akibat variasi pada parameter tertentu yang dapat dikontrol. Pada diagram bifurkasi, sumbu horizontal menunjukkan nilai parameter yang divariasikan.



Gambar 7. Bifurcation Diagram Hénon Map



Gambar 8. *Bifurcation Diagram Tinkerbell Map*



Gambar 9. *Bifurcation Diagram Tinkerbell-Hénon Map*

Berdasarkan Gambar 9, dapat dilihat bahwa Henon–Sine map tidak menunjukkan adanya kondisi periodik, melainkan memperlihatkan perilaku yang sangat kacau. Sebaliknya, pada Gambar 7 dan Gambar 8 terlihat bahwa Henon map dan Sine map menghasilkan pola perulangan yang semakin rumit seiring dengan meningkatnya nilai parameter. Namun demikian, terdapat rentang parameter tertentu yang menyebabkan nilai x yang dihasilkan menjadi kurang acak. Dengan demikian, Henon–Sine map memiliki kondisi chaos yang stabil pada rentang parameter yang lebih luas, yang mengindikasikan peningkatan ruang kunci (key space) dan menjadikannya lebih sesuai untuk digunakan dalam aplikasi kriptografi.

V. KESIMPULAN

Dalam makalah ini dikembangkan sebuah fungsi chaos baru yang merupakan hasil penggabungan antara Tinkerbell Map dan Hénon Map untuk keperluan pembangkitan bilangan acak semu. Fungsi yang diusulkan mampu menunjukkan kinerja yang lebih baik dengan menghasilkan deret bilangan yang memiliki tingkat keacakan lebih tinggi serta tingkat prediktabilitas yang lebih rendah. Evaluasi terhadap fungsi tersebut dilakukan melalui berbagai pengujian statistik, meliputi phase diagram untuk memvisualisasikan lintasan sistem, bifurcation diagram untuk menganalisis perubahan dinamika akibat variasi parameter. Hasil analisis ini memberikan pemahaman yang komprehensif mengenai sifat dan kinerja fungsi chaos yang dikembangkan, sekaligus memperkaya wawasan terkait karakteristik sistem chaos dan pemanfaatan bilangan acak semu dalam

bidang kriptografi.

UCAPAN TERIMAKASIH

Pertama-tama, penulis memanjatkan puji dan syukur atas kehadiran Tuhan Yang Maha Esa yang telah memberikan berkat dan rahmat yang tak terhingga, sehingga akhirnya penulis dapat menyelesaikan makalah ini dengan baik. Penulis mengucapkan terima kasih kepada semua pihak yang telah mendukung penulis dalam proses penulisan makalah ini. Khususnya kepada dosen pengampu Kriptografi IF4020, yaitu Bapak Rinaldi Munir yang telah mengajarkan dan membagi ilmunya yang diperlukan dalam penulisan makalah ini, beserta asisten yang telah membantu proses perkuliahan.

REFERENSI

- [1] Borah, M., Roy, P., & Roy, B. K. (2016). Synchronisation control of a novel fractional-order chaotic system with hidden attractor. In 2016 IEEE Students' Technology Symposium (TechSym). IEEE. <https://doi.org/10.1109/TechSym.2016.7872675>
- [2] Munir, Rinaldi. Pembangkit Bilangan Acak (Bahan Kuliah IF4020 Kriptografi)
- [3] Kocarev, L. Chaos-based cryptography: a brief overview. IEEE Circuits Syst. Mag. 1, 6–21. 2001.
- [4] Lambić, D., Nikolić, M.: Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn. 90, 223–232. 2017.

PERNYATAAN

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

Bandung, 24 Desember 2025

Dzaky Satrio Nugroho - 13522059