



ANALISIS DINAMIKA KOMPLEKS SISTEM MALASOMA DAN APLIKASINYA PADA SPEECH ENCRYPTION

*Aceng Sambas¹, Gugun Gundara¹, Mada Sanjaya², Mustafa Mamat³

¹Prodi Teknik Mesin, Fakultas Teknik

Universitas Muhammadiyah Tasikmalaya, INDONESIA

²Jurusan Fisika, Fakultas Sains dan Teknologi

Universitas Islam Negeri Sunan Gunung Djati Bandung, INDONESIA

³ Faculty of Informatic and Computing,

Universiti Zaenal Abidin, Kuala Terengganu, MALAYSIA

*E-mail: acengs@umtas.ac.id

ABSTRAK

Dengan perkembangan teknologi informasi dan komunikasi pengiriman keamanan data sangatlah diperlukan. Oleh karena itu, kami mengusulkan sistem enkripsi menggunakan sinyal chaos dengan inputan sinyal suara berdasarkan kombinasi dua sinyal yang berbeda. Untuk mendapatkan sinyal chaos yang baik, maka fenomena chaos yang dihasilkan oleh sistem Malasoma harus dipelajari secara intensif. Studi awal penelitian ini adalah menganalisis titik ekuilibrium, Lyapunov eksponen, Kaplan Yorke dan analisis peta Poincaré. Fokus terakhir makalah ini adalah aplikasi sinyal chaos dalam sistem keamanan komunikasi dengan input sinyal suara telah disajikan secara lengkap. Hasil enkripsi menggunakan pendekatan simulasi numerik Matlab menunjukkan bahwa sistem Malasoma sangat baik untuk dijadikan sistem keamanan data.

Kata kunci: Enkripsi Suara; Titik Ekuilibrium; Sistem Malasoma; Lyapunov Eksponen;

PENDAHULUAN

Chaos digunakan untuk menjelaskan perilaku kompleks dinamis tertentu, yaitu; sistem dengan keadaan variabel berubah terhadap waktu, yang mungkin akan menunjukkan dinamika yang sangat sensitif terhadap kondisi awal. Henri Poincaré adalah penemu

pertama chaos. Pada tahun 1890, saat mempelajari masalah “*the three-body problem*”, ia menemukan bahwa terdapat beberapa orbit yang non-periodik [1-2]. Perhatian dalam dinamika non linier dan dinamika chaos khususnya telah berkembang dengan pesat sejak tahun 1963, Edward Lorenz, ahli meteorologi MIT, ia merancang sebuah model 3-D untuk prediksi cuaca [3].

Dalam literatur, Sprott (1994) adalah orang pertama yang memperkenalkan aliran sederhana tanpa titik ekulibrium pada persamaan chaos yang telah dibuatnya [4], Pada tahun 2000, Malasoma mengusulkan persamaan Jerk *disipatif* sederhana dengan invarian keseimbangan [5], Sun dan Sprott (2009) membuat sirkuit Jerk dengan fungsi eksponensial [6], pada tahun 2010, Sprott membangun sistem 3-D dengan fungsi non linier sinusoidal hiperbolik [7], Pada tahun 2014, Chunbiao Li dan Sprott membangun sebuah sistem chaos non kuadrat tunggal [8] dan terakhir pada tahun 2015, Vaidyanathan menciptakan sistem chaos dengan dua fungsi nonlinier eksponensial [9]. Berdasarkan literature di atas, kami akan membangun sebuah generator pembangkit sinyal chaos dengan fungsi kubik.

Chaos telah banyak diterapkan untuk banyak disiplin ilmu, seperti ekologi [10], biologi [11], ekonomi [12], random bit generator [13], psikologi [14], Laser [15], astronomi [16], reaksi kimia [17], robotika [18-19], Teks enkripsi [20], enkripsi citra [21], enkripsi suara [22-25] dan sistem komunikasi yang aman [26-31].

Termotivasi oleh penelitian di atas, sistem Malasoma telah diusulkan dalam pekerjaan ini, pada bagian 2, kami menyajikan analisis sistem Malasoma menggunakan analisis Lyapunov eksponen, analisis Kaplan-Yorke, analisis peta Poincaré dan analisis numerik Runge-Kutta orde 4. Pada bagian 3, aplikasi sistem keamanan komunikasi data menggunakan sinyal chaos dan terakhir, bagian 4 berisi pernyataan kesimpulan.

MODEL MATEMATIKA DAN SIMULASI NUMERIK SISTEM MALASOMA

Malasoma menemukan bentuk fungsional kubik dari sistem dinamik tiga dimensi yang dapat menghasilkan fenomena chaos. Dinamika sistem dideskripsikan oleh persamaan di bawah ini [32]:

$$\ddot{x} = -a\dot{x} + x\dot{x}^2 - x \quad (1)$$

Dalam bentuk sistem, persamaan diferensial (1) dapat dinyatakan sebagai berikut:

$$\left. \begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -az + xy^2 - x \end{aligned} \right\} \quad (2)$$

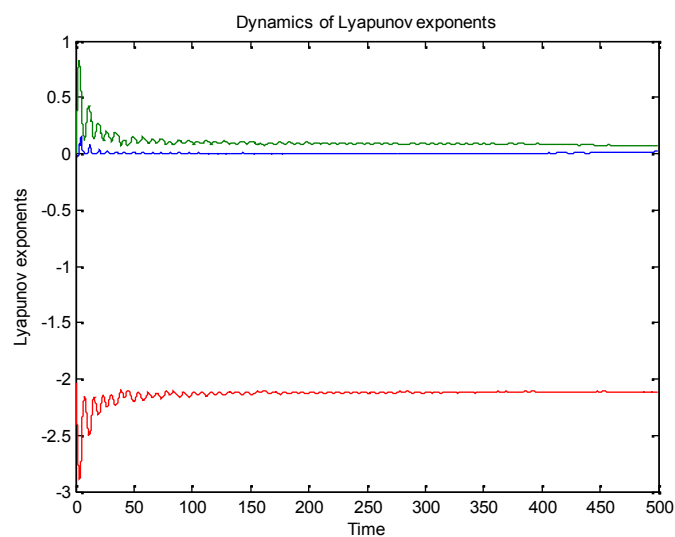
Di mana x , y , z adalah sebuah variabel dan ketika $a = 2.03$, sistem Malasoma pada persamaan (2) menunjukkan *strange attractor*, Kami telah memilih kondisi awal untuk sistem Malasoma $(x_0, y_0, z_0) = (0, 0.96, 0.1)$. Dari sistem Malasoma di atas diperoleh nilai Lyapunov eksponen di bawah ini;

$$L_1 = 0.0769, L_2 = 0, L_3 = -2.1069 \quad (3)$$

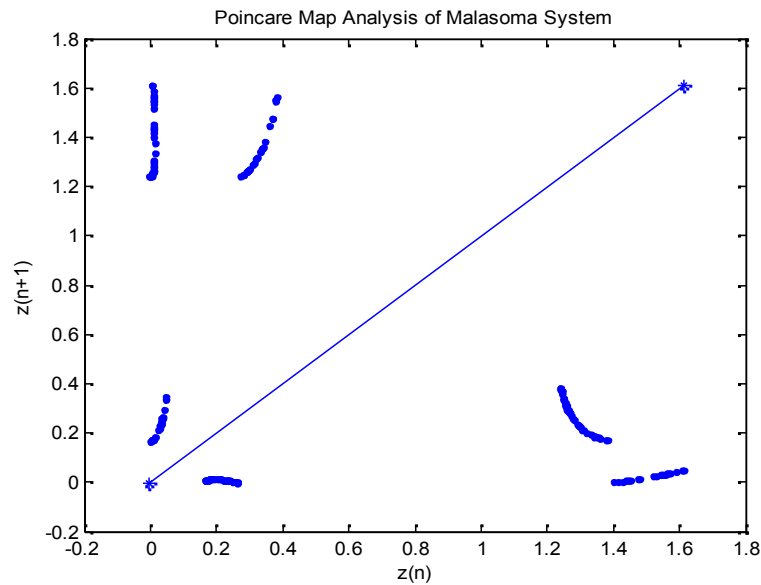
Dinamika Lyapunov eksponen di tunjukkan pada **Gambar 1**. Dengan demikian, maksimal Lyapunov eksponen (MLE) dari sistem Malasoma adalah $L_1 = 0,0769 > 0$. yang berarti bahwa sistem Malasoma memiliki perilaku chaos. Karena jumlah Lyapunov eksponen dalam persamaan (3) adalah nol, sistem Malasoma menunjukkan prilaku konservatif. Maka nilai dari analisis Kaplan Yorke ditunjukkan oleh perhitungan di bawah ini:

$$D_{KY} = 2 + \frac{L_1 + L_2}{|L_3|} = 2.0364 \quad (4)$$

Yang bersesuaian pecahan dimensi dari sistem pada persamaan (2) adalah $D_{KY} = 2,0364 > 2$. Oleh karena itu, sistem menunjukkan *strange attractor*. Selain itu, peta Poincare dari sistem pada **Gambar 2** juga mencerminkan sifat dari chaos.

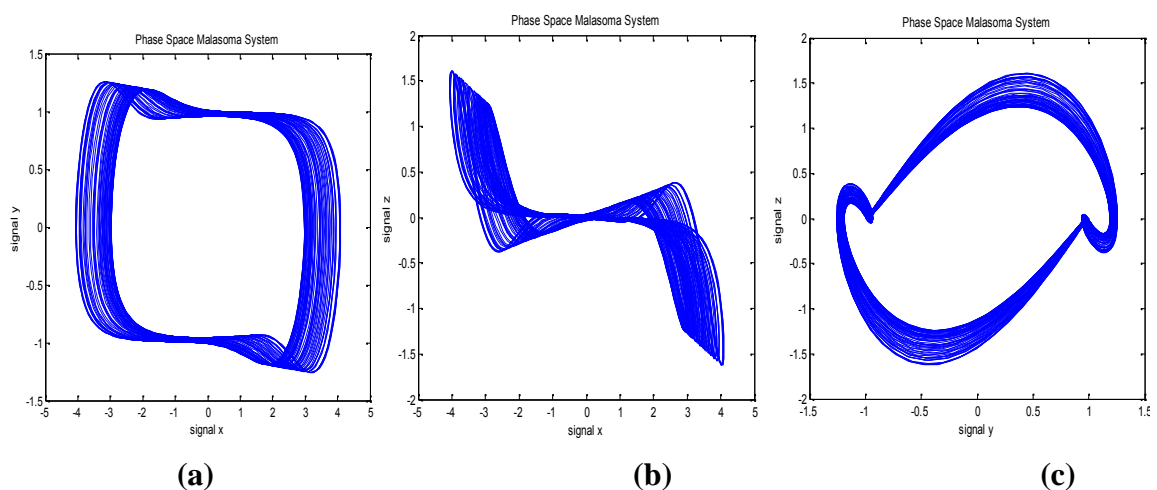


Gambar 1. Dinamika Lyapunov eksponen Sistem Malasoma untuk $a = 2.03$ menggunakan MATLAB 2010



Gambar 2. Peta Poincare pada bidang x - y - z ketika $a = 2.03$, menggunakan MATLAB 2010.

Untuk simulasi numerik dari sistem chaos didefinisikan oleh satu set persamaan diferensial, seperti sistem Malasoma pada persamaan (2), dapat digunakan teknik integrasi yang berbeda. Pada **Gambar 3 (a) - (c)** masing-masing menunjukkan proyeksi dari ruang orbit fase bidang x - y , bidang x - z dan bidang y - z . Untuk set parameter yang dipilih dan kondisi awal, sistem Malasoma pada persamaan (2) menyajikan *strange attractor* yang padat.



Gambar 3 Hasil simulasi numerik menggunakan MATLAB 2010, dengan $a = 2.03$ bidang xy , (b) bidang xz , (c) bidang yz .

ANALISIS TITIK EKUILIBRIUM

Sistem Malasoma memiliki satu titik ekuilibrium $E_0(0, 0, 0)$. Untuk titik ekuilibrium $(0, 0, 0)$, matriks Jacobi menjadi:

$$J(0,0,0) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & -2.03 \end{bmatrix} \quad (5)$$

Nilai-nilai eigen diperoleh dengan memecahkan persamaan karakteristik, $\det [J_1 - \lambda] = 0$ yaitu:

$$\lambda^3 + 2.03\lambda^2 - 1 = 0 \quad (6)$$

Dan diperoleh nilai eigen $\lambda_1 = -2.2309$, $\lambda_2, \lambda_3 = 0.1005 \pm 0.26619i$. Maka titik ekuilibrium yang sebenarnya adalah *saddle focus*, sehingga sistem pada persamaan (2) tidak stabil pada titik-titik ini.

APLIKASI SINYAL CHAOS PADA SPEECH ENCRYPTION

Dalam sistem keamanan komunikasi berbasis chaos, sinyal informasi dalam bentuk gelombang suara ditambahkan dengan sinyal chaos, kemudian ditransmisikan ke penerima melalui saluran publik. Karena sinyal yang ditransmisikan berupa sinyal chaos maka sistem ini dapat digunakan untuk keamanan data informasi yang dikirimkan. Selanjutnya sinyal yang dikirim ke publik akan diterima oleh *receiver* yang identik dengan *transmitter*-nya, dan sinyal chaos dipisahkan dari data atau informasi yang dikirimkan menggunakan *subtractor*. Keberadaan sinyal chaos diantara *receiver* dan *transmitter* menunjukkan bahwa sistem chaos sangat baik digunakan dalam enkripsi data.

Penjumlahan sinyal informasi (gelombang suara) dan sinyal chaos, yang dihasilkan oleh sistem Malasoma adalah enkripsi sinyal baru $m_{\text{encryption}}(t)$, yang diberikan oleh Persamaan. (7)

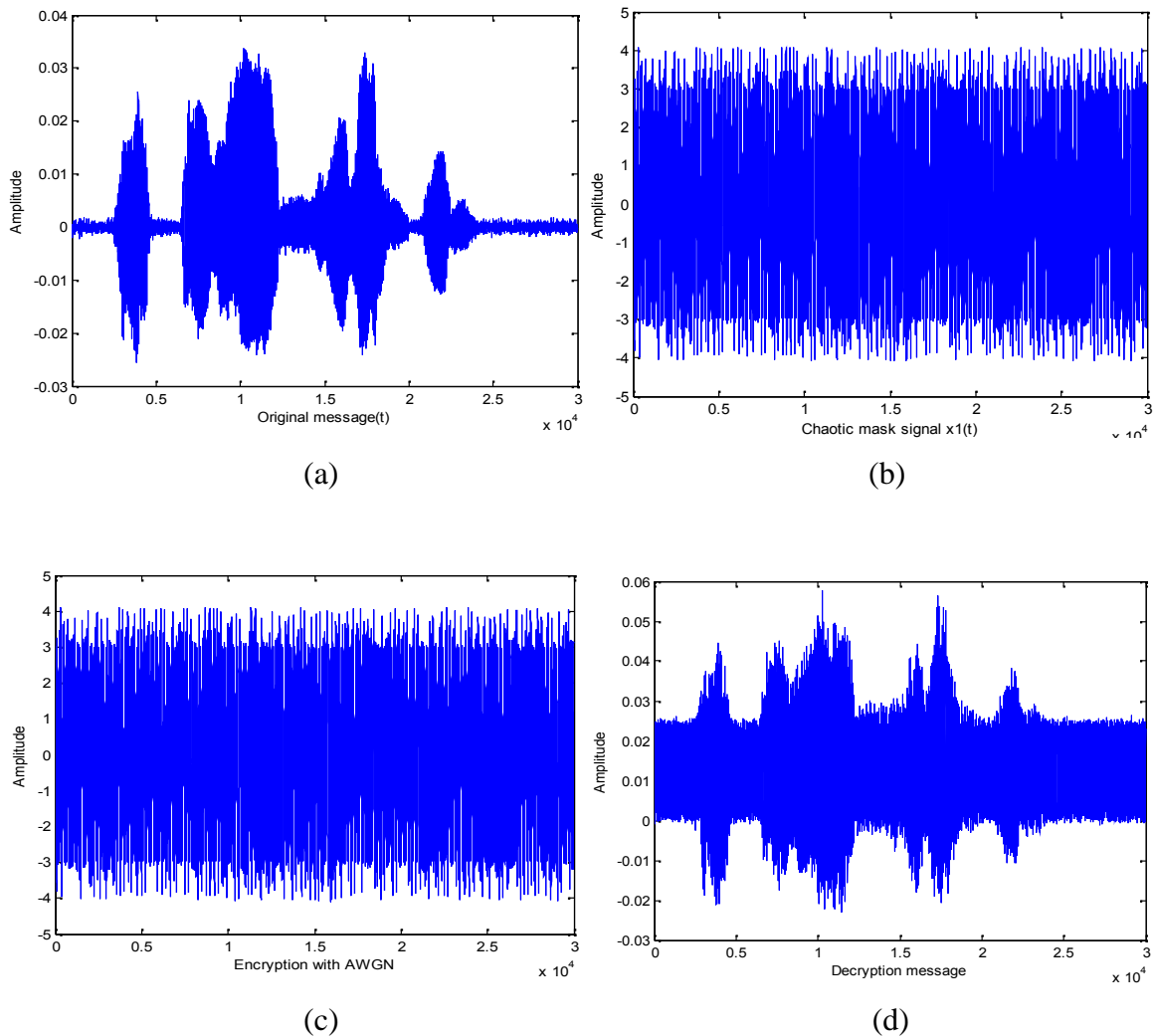
$$m_{\text{encryption}}(t) = m_{\text{informasi}}(t) + m_{\text{sinyal chaos}}(t) + n(t) \quad (7)$$

$m_{\text{informasi}}(t)$ adalah sinyal pesan dalam bentuk gelombang suara, $m_{\text{sinyal chaos}}(t)$ adalah sinyal chaos yang digunakan yaitu sistem Malasoma pada persamaan (1) dan $n(t)$ adalah *AWGN noise* yang datang dari saluran kabel. Setelah menyelesaikan proses enkripsi sinyal asli dapat dipulihkan dengan prosedur berikut.

$$m_{\text{decryption}}(t) = m_{\text{encryption}}(t) - m_{\text{sinyal chaos}}(t) \quad (8)$$

Sinyal $m_{\text{decryption}}(t)$ adalah sinyal baru yang telah terpisah dari sinyal chaos dengan menggunakan subtraktor. Fakta bahwa sinyal input sama dengan sinyal output maka sinyal chaos dalam hal ini yaitu sistem Malasoma sangat baik dijadikan enkripsi data.

Dengan bantuan MATLAB, gelombang suara dengan lafal “Assalamua’laikum” diambil untuk digunakan sinyal informasi dengan frekuensi sampel 11025Hz seperti yang terdapat pada **Gambar 4**.



Gambar 4. Data sistem komunikasi menggunakan chaos: (a) Pesan asli (b) Chaos masking (c) enkripsi dengan AWGN (d) Pesan diterima

Pengolahan sinyal yang dihasilkan pada **Gambar 4a** Merupakan Pesan asli untuk memberitahukan informasi yang dikirimkan oleh *transmitter* kepada *receiver*. Pada **Gambar 4b** Merupakan *Chaos masking* untuk menutupi pesan asli, agar pesan asli tidak terdeteksi oleh *receiver* lain yang tidak berhubungan dengan informasi yang akan dikirim

tersebut. Pada **Gambar 4c** Hasil dari pesan asli yang sudah digabungkan dengan sinyal chaos akan menghasilkan gelombang suara yang lebih rapat dan akan dikirimkan kepada *receiver*, dalam bentuk file. Pada **Gambar 4d** Merupakan informasi yang sudah diterima oleh receiver, dengan gelombang suara yang sama dengan pesan asli, sebelum ditambahkan oleh sinyal chaos.

KESIMPULAN

Setelah dianalisis, pada Generator pembangkit sinyal chaos telah ditemukan, titik ekuilibrium yang berada pada sistem Malasoma, yaitu *saddle focus* yang telah dianalisis dengan menggunakan persamaan Jacobi yang menghasilkan Lyapunov eksponen. Dengan analisis menggunakan Kaplan-Yorke, Lyapunov eksponen, peta Poincaré dan numerik Runge-Kutta orde 4, telah mencerminkan sifat dari sinyal chaos. Dari sifat chaos tersebut, dengan menggunakan *speech encryption* akan menghasilkan gelombang suara untuk mengirimkan informasi yang hanya akan terhubung dengan *receiver* yang sudah dikenal. Sifat-sifat dasar dari sistem seperti titik ekuilibrium, Lyapunov eksponen, Kaplan Yorke dan peta Poincaré serta potret fase yang dijelaskan secara rinci menunjukkan perilaku chaos. Selain itu, telah ditunjukkan bahwa sistem malasoma ini sangat baik digunakan untuk *speech encryption*. Dalam penelitian selanjutnya, kita dapat menerapkan sistem Malasoma ini dalam aplikasi praktis seperti robot, random bits Generator dan sistem keamanan komunikasi.

REFERENSI

- [1] H. Zhang, "Chaos Synchronization and Its Application to Secure Communication," PhD Thesis, University of Waterloo, Canada, 2010.
- [2] J. H. Poincaré, Sur le problme des trois corps et les quations de la dynamique. divergence des sries de m. lindstedt, *Acta Mathematica*, vol. 13, no. 3, 1890, 1–270.
- [3] E.N. Lorenz, Deterministic Nonperiodic Flow. *J. of the Atmospheric Sciences*, vol. 20, pp. 130-141, 1963.
- [4] J. C. Sprott, Some Simple Chaotic Flows, *Phys. Let. E*, vol. 50, pp. 647-650, 1994.
- [5] J. M. Malasoma, A New Class of Minimal Chaotic Flows, *Phys. Lett.A*, vol. 264, pp. 383-389, 2000.
- [6] K. H Sun dan J. C. Sprott, A Simple Jerk System With Piecewise Exponential

- Nonlinearity, *International Journal of Nonlinear Sciences and Numerical Simulation*, vol. 10, pp. 1443-1450, 2009.
- [7] J. C. Sprott, *Elegant Chaos Algebraically Simple Chaotic Flows*, Singapore: World Scientific, 2010.
- [8] C. Li dan J. C. Sprott, Chaotic flows with a single nonquadratic term, *Physics Letter A*, vol. 378, pp. 178–183, 2014.
- [9] S. Vaidyanathan, Ch. K. Volos, I. M. Kyprianidis, I. N. Stouboulos dan V. T. Pham, Analysis, Adaptive Control and Anti-Synchronization of a Six-Term Novel Jerk Chaotic System with two Exponential Nonlinearities and its Circuit Simulation. *Journal of Engineering Science and Technology Review*, vol. 8, no. 2, pp. 24-36, 2015.
- [10] M. Sanjaya W. S, I. Mohd, M. Mamat dan Z. Salleh, Mathematical Model of Three Species Food Chain Interaction with Mixed Functional Response. *International Journal of Modern Physics: Conference Series*, vol. 9, pp. 334–340, 2012.
- [11] M. Sanjaya W. S, M. Mamat, Z. Salleh, dan I. Mohd, Bidirectional Chaotic Synchronization of Hindmarsh-Rose Neuron Model, *Applied Mathematical Sciences*, vol. 5, no. 54, pp. 2685 – 2695, 2011.
- [12] S. Bouali, A. Buscarino, L. Fortuna, M. Frasca, dan L. V. Gambuzza, Emulating Complex Business Cycles by Using an Electronic Analogue, *Nonlinear Analysis: Real World Applications*, vol. 13, pp. 2459–2465, 2012.
- [13] Ch. K Volos, I. M. Kyprianidis dan I. N. Stouboulos, Text Encryption Scheme Realized with a Chaotic Pseudo-Random Bit Generator, *Journal of Engineering Science and Technology Review*, vol. 6, pp. 9-14, 2013.
- [14] J. C. Sprott., Dynamical models of love, *Nonlinear Dyn. Psych. Life Sci.*, vol. 8, pp. 303–314, 2004.
- [15] N. Li, W. Pan, L. Yan, B. Luo, dan X. Zou, Enhanced chaos synchronization and communication in cascade-coupled semiconductor ring lasers, *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, pp. 1874-1883, 2014.
- [16] D. W. Moore dan E. A. Spiegel, A Thermally Excited Non-Linear Oscillator, *Astrophys. J*, vol. 143, pp. 871-887, 1986.
- [17] M. Kyriazis, Applications of chaos theory to the molecular biology of aging, *Experimental Gerontology*, vol. 26, pp. 569-572, 1991.

- [18] A. Sambas., S. Vaidyanathan., M. Mamat., M. Sanjaya WS., dan D. S. Rahayu, (2016). A 3-D Novel Jerk Chaotic System and Its Application in Secure Communication System and Mobile Robot Navigation. *In Advances and Applications in Chaotic Systems* (pp. 283-310). Springer International Publishing.
- [19] M. Sanjaya WS, A. Sambas dan M. Mamat, Analisis Dinamika Sirkuit Chaos 3-D Autonomous serta Aplikasinya untuk Navigasi Mobile robot, *Jurnal ISTEK*, vol. 8, no. 1, pp. 47-64, 2014.
- [20] Ch. K Volos, I. M. Kyprianidis dan I. N. Stouboulos, Text Encryption Scheme Realized with a Chaotic Pseudo-Random Bit Generator, *Journal of Engineering Science and Technology Review*, vol. 6, pp. 9-14, 2013.
- [21] A. S Andreatos dan A. P. Leros, Secure Image Encryption Based on a Chua Chaotic Noise Generator, *Journal of Engineering Science and Technology Review*, vol. 6, pp. 90-103, 2013
- [22] A. Sambas., M. Mamat., M. Sanjaya WS dan S. Vaidyanathan., Model Matematik dan Analisis Sirkuit Genesio-Tesi dalam Sistem Keamanan Komunikasi Suara. *ALHAZEN Journal of Physics*, vol 2, no. 1, pp. 58-69, 2015.
- [23] M. Abdulkareem dan I. Q. Abduljaleel I. Q, Speech Encryption using Chaotic Map and Blowsh Algorithms, *Journal of Basrah Researches.*, vol. 39, pp. 68-76, 2013.
- [24] M. Ashtiyani., P. Moradi Birgani dan S. S. Karimi Madahi, Speech Signal Encryption Using Chaotic Symmetric Cryptography, *Journal of Basic and Applied Scientific Research*, vol 2, no. 2, pp. 1678-1684, 2012.
- [25] K. W. Tang, and W. K. S. Tang, A Chaos-based Secure Voice Communication System, *International Conference on Industrial Technology*, pp. 571–576, 2005.
- [26] A. Sambas., M. Sanjaya W.S. dan Halimatussadiyah, Unidirectional Chaotic Synchronization of Rossler Circuit and Its Application for Secure Communication, *WSEAS Transactions on Systems*, vol. 9, no. 11, pp. 506 – 515, 2012.
- [27] A. Sambas, M. Sanjaya W. S dan Halimatussadiyah, Unidirectional Chaotic Synchronization of Rossler Circuit and Its Application for Secure Communication”. *WSEAS Transaction On System*, vol. 11, pp. 506-515, 2012.
- [28] Aceng Sambas, Mada Sanjaya W. S., M. Mamat, N. V Karadimas dan O. Tacha, Numerical Simulations in Jerk Circuit and It’s Application in a Secure Communication System. *Recent Advances in Telecommunications and Circuit Design. WSEAS 17th International Conference on Communications Rhodes Island, Greece July 16-19, 2013*, 190-196, ISBN: 978-960-474-310-0.
- [29] Aceng Sambas, Mada Sanjaya W. S., dan M. Mamat., Design and Numerical Simulation of Unidirectional Chaotic Synchronization and Its Application in Secure Communication

- System. *Recent Advances in Nonlinear Circuits: Theory and Applications. Journal of Engineering Science and Technology Review.*, vol 6, no. 4, pp. 66-73, 2013.
- [30] Aceng Sambas, Mada Sanjaya W. S., dan M. Mamat, Bidirectional Coupling Scheme of Chaotic Systems and its Application in Secure Communication System, *Journal of Engineering Science and Technology Review*, vol. 8, no. 2, pp. 89 – 95, 2015.
- [31] Aceng Sambas, Mada Sanjaya W. S., dan M. Mamat, Z. Salleh and F. S. Mohamad, Secure Communications Based on the Synchronization of the New Lorenz-like Attractor Circuit, *Advanced Studies in Theoretical Physics*, vol. 9, no. 8, pp. 379 – 394, 2015.
- [32] J. M. Malasoma, What is the simplest dissipative chaotic jerk equation which is parity invariant ? *Phys. Lett. A*, vol. 264, pp. 383-389, 2000.