ALGORITMA OPTIMASI CHAOS PADA HOPFIELD NETWORK MODIFIKASI UNTUK PERSAMAAN NONLINEAR

Rina Pramitasari

Teknik Komputer Universitas AMIKOM Yogyakarta
email : rina.pramitasari@amikom.ac.id

Abstraksi

Kriptanalisis dapat digunakan untuk menguji keamanan kriptografi. Keamanan kriptografi ada pada sulitnya memecahkan permasalahan matematika. Pada kriptografi kunci public salah satunya adalah mencari akar untuk menyelesaikan persamaan polynomial. Penelitian ini dilakukan dengan menerapkan Algoritma Optimasi Chaos dan Hopfield Network Modifikasi. Hasil penelitian menunjukkan Algoritma Optimasi Chaos dan Hopfield Network Modifikasi lebih baik dari pada Newton Raphson. Karena nilai awal yang diberikan pada Hopfield Network Modifikasi selalu dekat dengan solusi dan memberi hasil yang akurat.

***Kata Kunci* :**
Algoritma Optimasi Chaos, Hopfield Network Modifikasi, Persamaan Nonlinear.

Abstract

Cryptoanalysis can be used to test cryptographic security. Cryptographic security lies in the difficulty of solving mathematical problems. In public key cryptography, one of them is to find the root to solve polynomial equations. This research was conducted by applying Chaos Optimization Algorithm and Modified Hopfield Network. The results showed that the Chaos Optimization Algorithm and Hopfield Network Modification were better than Newton Raphson. Because the initial value given to the Hopfield Network Modification is always close to the solution and gives accurate results..

***Keywords* :**
Chaos Optimization Algorithm, Modified Hopfield Network, Nonlinearl Equation

1. Pendahuluan

Komputer sedang mengalami perkembangan menuju komputer quantum. Kriptografi harus dapat mengimbangi dan sejalan dengan komputer quantum. Ada beberapa kandidat yaitu *Lattice - Based Cryptography*, *Code - Based Crytography*, *Multivariate - Based Crytography*. Sistem Kriptografi kunci public menggunakan dua jenis kunci, yaitu kunci public dan kunci rahasia. Keamanan kriptografi ada pada sulitnya memecahkan permasalahan matematika. Kriptanalisis dapat digunakan untuk menguji keamanan kriptografi [4][5].

Tingkat keamanan sistem kriptografi kunci publik multivariate adalah pada menyelesaikan system persamaan polynomial multivariable kuadratik yang disebut MQ-problem (multivariate quadratic problem) [4][5].

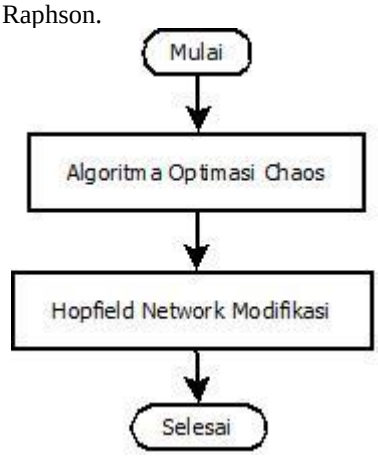
Mencari akar system persamaan nonlinear sederhana bisa menggunakan metode analitik. Sedangkan untuk system persamaan nonlinear kompleks dimana sering ditemui dikehidupan nyata, bisa menggunakan metode numerik. Kelemahan metode numerik harus memenuhi syarat dekat dengan solusi untuk bisa mendapatkan iterasi yang konvergen. Maka untuk menyelesaikan tersebut dipilih jaringan syaraf tiruan dimana sebuah prosesor yang terdistribusi parallel dan mempunyai kecenderungan untuk menyimpan pengetahuan yang didapatkannya dari pengalaman dan membuatnya tetap tersedia untuk digunakan [8].

Jaringan Hopfield pertama kali diperkenalkan John Hopfield. Jaringan Hopfield adalah pelatihan terbimbing yang terhubung penuh, dimana setiap neuron terhubung dengan neuron lainnya. Hasil pengujian didapat jika diberikan nilai awal jauh dari solusi dan kompleksnya persamaan nonlinear, maka tidak mendapatkan hasil yang akurat [3][6][7].

Untuk mengatasi tersebut nilai awal menggunakan Algoritma Optimasi Chaos dengan menerapkan persamaan logistic. Dengan asumsi, sensitive terhadap kondisi awal adalah dimana perubahan kecil disuatu tempat dalam system nonlinear dapat mengakibatkan perbedaan besar pada keadaan berikunya. Masalah dalam minimum global adalah tidak mungkin menentukan apakah solusi terbaik saat ini terletak di minimum local atau global jika konvergensi sudah diterima. Dengan kata lain, biasanya tidak jelas apakah proses minimum dapat dihentikan, apakah harus berkonsentrasi pada perbaikan minimum saat ini, ataukah harus memeriksa bagian-bagian ruang pencarian pengganti yang lain. Dan menjadi lebih rumit jika ada beberapa minimum local [1][2][9][10][11].

2. Metode Penelitian

Langkah penelitian yang akan dilakukan disajikan pada Gambar 1 berikut. Pertama menggunakan Algoritma Optimasi Chaos untuk menghasilkan nilai output. Kemudian nilai output digunakan pada nilai awal Hopfield Network Modifikasi untuk persamaan polynomial. Kemudian dibandingkan dengan Newton Raphson.



Gambar 1 Langkah Penelitian

2.1. Persamaan Nonlinear

Salah satu persamaan nonlinear adalah persamaan polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

2.2. Algoritma Optimasi Chaos

a. Hitung normalisasi data pada [0,1]

$$N' = \frac{N - N_{min}}{N_{max} - N_{min}} \quad (2)$$

Dimana
N' = Data sudah normal
N = Data belum normal
N_{max} = Data besar
N_{min} = Data kecil

b. Proses pertama, Inisialisasi r = 0, iterasi maksimum = r max. $A_i^0 \in (0,1)$, $A_i^0 \neq (0, 0.25, 0.5, 0.75, 1)$. Tetapkan nilai $A^* = 0$, $X^* = 0$ dan F^* dengan nilai besar.

c. Hitung chaos A_i^r ke dalam rentang optima $X_i^r \in [a^1, b^1]$

$$X_i^r = a^1 + A_i^r (b^1 - a^1) \quad (3)$$

Dimana
X_i^r = optima ke-r
A_i^r = chaos ke-r
a^1 = interval bawah pertama
b^1 = interval atas pertama

d. Hitung fungsi objek $F(X^r)$ dengan MSE
Jika $F(X^r) < F^*$ maka $A^* = A^r$, $X^* = X^r$ dan $F^* = F(X^r)$.
Jika $F(X^r) \geq F^*$ maka diam X^r

e. Hitung chaos

$$A_i^{r+1} = \mu A_i^r (1 - A_i^r) \quad (4)$$

Dimana
A_i^{r+1} = chaos ke-r+1
A_i^r = chaos ke-r
μ = 4

f. Jika r kurang $r\ max$, maka ulangi langkah b – e. Jika lebih, maka lanjut ke langkah g.

g. Proses kedua. Hitung chaos A_i^h ke dalam rentang optima $X_i^h \in [a^2, b^2]$

$$X_i^h = X_i^* + \omega \left(2 * A_i^h - 1\right), i = 1, 2, \ldots, n \quad (5)$$
$$\omega = \rho(b^2 - a^2), \ \rho \in (0,\ 0.5)$$

Dimana
X_i^h = optima ke-h
A_i^h = chaos ke-h
a^2 = interval bawah kedua
b^2 = interval atas kedua
ρ = faktor ruang sempit, ρ = 0,4

h. Hitung fungsi objek $F(X^h)$ dengan MSE
Jika $F(X^h) < F^*$ maka $A^* = A^h$, $X^* = X^h$ dan $F^* = F(X^h)$.
Jika $F(X^h) \geq F^*$ maka diam X^h

i. Hitung chaos

$$A_i^{h+1} = \mu A_i^h \left(1 - A_i^h\right) \quad (6)$$

Dimana
A_i^{h+1} = chaos ke-h+1
A_i^h = chaos ke-h
μ = 4

j. Jika h kurang $h\ max$, maka ulangi langkah g –i
Jika lebih maka COA berakhir dan X^* = solusinya.

2.3. Hopfield Network Modifikasi

a. Mengubah persamaan polynomial menjadi fungsi energy

$$g_1(.) = Ax + B \quad (7)$$

$$E = -\frac{1}{2}\sum_{i=1}^{m}(g_i(.))^2$$

b. Turunkan fungsi energy

$$\frac{\partial E}{\partial x} \quad (8)$$

c. Sesuaikan dengan persamaan Hopfield

$$\frac{du_j}{dt} = W_1 x + l_{bias} \quad (9)$$

d. Hitung $u(t)$dengan metode Euler

$$u(t+1) = u(t) + \Delta t(W_1 x + l_{bias}) \quad (10)$$

e. Update nilai $x(t)$

$$x(t) = \frac{1}{1 + e^{-u(t)}} \quad (11)$$

f. Sampai syarat terpenuhi

3. Hasil dan Pembahasan

Penelitian menggunakan pemrograman Python. Data pengujian menggunakan persamaan polynomial. Data uji ada 3 persamaan yaitu
Persamaan 1 dengan solusi 0.17

$$x^4 + x^3 - 0.0289x - 0.00083521 = 0$$

Persamaan 2 dengan solusi 0.57

$$x^4 + x^3 - 0.3249x - 0.10556001 = 0$$

Persamaan 3 dengan solusi 0.97

$$x^4 + x^3 - 0.9409x - 0.88529281 = 0$$

Pada algoritma optimasi chaos. r max = 5000, h max = 10000 dan rentang sempit p = 0.1. Interval pertama = [-50, +50] dan interval kedua = [-2, +2]. Kemudian menggunakan Hopfield Network Modifikasi.

Tabel 1 Hasil Uji Dengan Persamaan 1

X akhir	Iterasi	Error
0.1736576477	11933	0.0

Tabel 2 Hasil Uji Dengan Persamaan 2

X akhir	Iterasi	Error
0.5699981627	36	0.0

Tabel 3 Hasil Uji Dengan Persamaan 3

X akhir	Iterasi	Error
0.9699990854	14	0.0

Tabel 1 sampai 3 adalah hasil uji dengan metode yang diusulkan

Tabel 4 Hasil Uji Newton Raphson Dengan Persamaan 1

X1	X akhir	Iterasi	Error
-2.29	-	-	-
0.29	0.1699999999999998	6	7.139171460615693e-17
2.29	0.1699999999999998	13	-1.5398212954269154e-17

Tabel 5 Hasil Uji Newton Raphson Dengan Persamaan 2

X1	X akhir	Iterasi	Error
-2.29	-	-	-
0.29	0.57	14	4.989956581829081 5e-17-
2.29	0.57	9	4.989956581829081 5e-17

Tabel 6 Hasil Uji Newton Raphson Dengan Persamaan 3

X1	X akhir	Iterasi	Error
-2.29	-	-	-
0.29	-	-	-
2.29	0.97	8	-0.0

Pada Tabel 4 sampai 6 menunjukkan hasil uji dengan metode Newton Raphson

4. Kesimpulan

Berdasarkan hasil penelitian Algoritma Optimasi Chaos dan Hopfield Network Modifikasi yang telah dilakukan berhasil mencari akar solusi. Tingkat keberhasilan tersebut dipengaruhi oleh beberapa factor. Kekurangan Hopfield Network Modifikasi adalah nilai awal yang jauh dari solusi dan kompleksnya persamaan polynomial, tidak akan mendapatkan hasil yang akurat. Kelemahan tersebut dapat diatasi dengan menggunakan Algoritma Optimasi Chaos, dimana dapat mengatasi terjebak ke dalam minimum local. Dimana hal ini efisien. Kemudian dibandingkan dengan Newton Raphson. ketika nilai awal yang diberikan tidak dekat dengan solusi, maka menghasilkan pengujian iterasi divergen. Oleh karena itu, nilai awal harus dekat dengan solusi, maka menghasilkan pengujian iterasi konvergen. Dimana hal ini tidak efisien.

Daftar Pustaka

[1] Alligood, K. T., Sauer T. D., Yorke J. A., 1996, Chaos (An Introduction to Dynamical Systems), Springer, New York.
[2] Ammaruekarat, P., Meesad, P., 2011, A Chaos Search for Multi-Objective Memetic Algorithm, International Conference on Information and Electronics Engineering IPCSIT vol.6 (2011) IACSIT Press, Singapore.
[3] D. Mishra, P. K. Kalra, Modified Hopfield Neural Network Approach for Solving Nonlinear Algebraic Equations, Engineering Letters, 14:1, EL_14_1_23 (Advance online publication: 12 February 2007)
[4] J. Ding, J. E. Gower, dan D. S. Schmidt, 2006, Multivariate Public Key Cryptosystem, Springer, USA.
[5] M. Z. Riyanto, "Sistem Kriptografi Kunci Publik Multivariat", Seminar Nasional Matematika dan Pendidikan Matematika, 27 November 2010 Jurusan pendidikan Matematika FMIPA UNY.

[6] M. M. Gupta, L. Jin, N. Homma, 2003, Static and Dynamic Neural Networks, From Fundamentals to Advanced Theory, John Wiley & Sonsm Inc., Hoboken, New Jersey.
[7] P. Rina, Kombinasi Backpropagation dan Hopfield Modifikasi untuk Persamaan Polynomial, ULTIMATICS, Vol. XII, No. 1, Juni 2020.
[8] R. Munir, Metode Numerik, Bandung: Informatika, 2008.
[9] Ridwan, A., 2006, Dinamika Fraktal dan Chaos, Istitut Teknologi Bandung, Bandung.
[10] Hui-juan, L., Huo-ming, Z., Long-hua, M., 2006, A new optimization algorithm based on chaos, Journal of Zhejiang University SCIENCE A. ISSN 1009-3095 (Print); ISSN 1862-1775 (Online).
[11] Weise, T., 2009, Global Optimization Algorithm Theory and Application, http://www.it-weise.de/, 26-06-2009.