Penerapan Multi Logistic Map dalam Algortima Enkripsi Citra Digital

Edi Sukirman, Suryadi M.T., Eva Nurpeti, Dhian Widya dan Wiwit Widhianto

Jurusan Sistem Informasi, Universitas Gunadarma
Departemen Matematika Universitas Indonesia, Jakarta, Indonesia
sukirman@staff.gunadarma.ac.id

Abstrak

Penelitian ini membahas mengenai proses pengiriman data secara acak (enkripsi) sehingga tidak dapat dibaca oleh pihak lain, pengiriman data tersebut haruslah menyertakan kunci sehingga data yang yang dinamakan deskripsi, agar tidak bocor kepada pihak yang tidak bertanggung jawab maka dibuatlah user id dan password dengan menggunakna algoritma RSA, Tujuan penelitian ini adalah menjaga keamanan data agar tidak digunakan oleh pihak yang tidak berkepentingan, metode penelitian ini adalah studi literature, dengan hasil penelitian ini adalah data yang dikirimkan terlebih dahulu di enkripsikan dan data yang telah di enkripsikan maka menyediakan kunci sebagai deskripsi sehingga informasi tersebut tidak terlihat oleh pihak lain. Citra digital merupakan salah satu bentuk informasi yang sering dijadikan sasaran kejahatan. Sehingga dibutuhkan teknik yang handal, aman, dan cepat guna pengamanannya. Untuk itu dirancang suatu algoritma enkripsi citra digital yang dapat meningkatkan daya tahan terhadap brute force attack. Algoritma enkripsi tersebut menggunakan *multi logistic map* sebagai pembangkit bilangan acak untuk key stream. Formulasi nilai acak gabungannya menggunakan aturan *product of sum* (POS) dari kombinasi dua dari tiga nilai x_i masing-masing dari tiga *logistic map*. Diperoleh dari hasil pengujian yaitu ruang kuncinya mencapai 10^{90} dan sensitivitas kuncinya mencapai 10^{-20}. Sehingga menjadikan algoritma ini sangat sulit dipecahkan oleh *brute force attack*.

Kata Kunci : Algoritma enkripsi, citra digital, multi logistic map.

Pendahuluan

Pembahasan dalam paper ini yakni terkait dengan usaha untuk mengenkripsi suatu citra digital dengan menerapkan suatu metode selain metode Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan Rivest-Shamir-Adleman Algorithm (RSA). Hal tersebut dilakukan sebagai salah satu alternatif dengan harapan akan dapat memnghasilkan waktu komputasi yang lebih baik. Menurut Stallings, dalam algoritma enkripsi citra digital yang lebih diutamakan adalah enkripsi citra digital yang memakan waktu lebih cepat tanpa mengorbankan keamanannya [1]. Metode yang digunakan dalam proses enkripsi citra dalam paper ini yakni metode yang berbasis chaos, yang telah banyak dikaji oleh banyak peneliti karena memiliki kinerja yang baik dalam tingkat keamanan dan kompleksitasnya [2-17]. Secara khusus ide dari metodenya mengacu pada metode yang dilakukan oleh Suryadi dkk dan juga Munir [11, 12, 13, 14] dengan menggunakan jenis fungsi chaosnya adalah fungsi logistic map. Fungsi logistic map didefinisikan sebagai fungsi $L_\lambda : R \to R$, $L_\lambda(x) = \lambda x(1-x)$ yang merupakan fungsi satu variabel x dan λ adalah parameter yang tetap. Variabel x berada dalam interval [0,1] dan parameter λ nilainya pada interval (0,4] dan adapun penyajian logistic map tersebut dalam bentuk iteratifnya adalah :

$$x_{n+1} = \lambda x_n(1-x_n) \qquad (1)$$

dengan $n = 0, 1, 2, 3 \ldots$.dan x_0 adalah nilai awal iterasinya [2,3,5]

Dalam paper ini algoritma enkripsinya dibuat dengan menerapkan multi logistic map yakni menggunakan tiga logistic map dengan formula nilai acak gabungannya dalam format *product of sum* (POS). sedangkan peneli-

tian lainnya menggunakan format *sum of product* (SOP) [13]. Adapun pengujian algoritmanya dilakukan untuk melihat ketahanannya terhadap serangan *brute force* dengan mengacu pada analisis ruang kunci. Selain itu juga akan dipertimbangkan rata-rata waktu proses enkripsi dan dekripsi.

Algoritma Enkripsi Citra Multi Logistic map

Algoritma enkripsi citra digital dalam paper menggunakan tiga *logistic map* yang diproses secara simultan yang bentuknya seperti persamaan (1). Input dari algoritma ini adalah citra asli dan kunci, kunci tersebut yaitu x_0 dan λ untuk masing-masing persamaannya, sehingga total ada 6 parameter input. Sedangkan outputnya adalah citra yang telah terenkripsi. Untuk mengakses kembali citra asli kita maka dilakukanlah proses dekripsi yang merupakan proses kebalikan (invers) dari proses enkripsi. Input pada proses dekripsi adalah citra yang telah terenkripsi dan kunci. Kunci yang digunakan dalam proses dekripsi adalah sama pada saat proses enkripsi, agar didapat kembali informasi (citra) aslinya. Algoritma enkripsinya, mengacu pada penelitian sebelumnya [11, 12, 13], dengan perbedaannya adalah dalam paper ini formula nilai acak gabungannya menggunakan format POS yaitu $x_i^G = (x_i^{(1)} + x_i^{(2)}).(x_i^{(2)} + x_i^{(3)}).(x_i^{(1)} + x_i^{(3)})$.

Hasil dan Analisis Uji Coba

Data uji yang digunakan adalah citra digital berwarna yang bernama cat.jpg, dengan berbagai ukuran yang disajikan pada Tabel 1.

Tabel 1: Citra Data Uji cat.jpg

Data Uji	Nama dan tampilan Citra	Ukuran Citra (piksel)	Ukuran Citra (byte)
1		64 × 47	2,71 K
2		128 × 94	5,69 K
3		256 × 188	13,4 K
4		512 × 376	35,3 K

Semua data uji pada Tabel 1 akan digunakan dalam proses enkripsi untuk diperlihatkan waktu proses enkripsi dan dekripsi dari algoritma dalam paper ini. Kemudian akan dilakukan pengujian daya tahan terhadap brute force attack dengan analisis sensitivitas kunci dan penentuan ukuran ruang kunci. Namun sebelumnya akan dianalisis terhadap rata-rata waktu enkripsi dan dekripsinya.

Analisis Waktu Enkripsi dan Dekripsi

Pengujian terhadap semua data uji citra digital, dilakukan dengan menggunakan nilai kunci yang sama, baik untuk proses enkripsi maupun dekripsi. Nilai awal (kunci) yang digunakan adalah $x_0^{(1)} = 0.1$, $x_0^{(2)} = 0.2$, $x_0^{(2)} = 0.3$ dan dengan nilai λ=4 yang sama untuk ketiganya. Berdasarkan hasil pengujian terhadap seluruh data uji citra digital, didapatkan hasil rata-rata waktu enkripsi dan dekripsi yang terlihat pada Tabel 2 dari masing-masing 10 kali percobaan.

Tabel 2: Rata-rata Waktu Proses Enkripsi dan Dekripsi Citra cat.jpg

Data Uji	Ukuran Citra (piksel)	Rata-rata waktu enkripsi (detik)	Rata-rata waktu dekripsi (detik)
1	64 × 47	0.30299	0.22500
2	128 × 94	0.85400	0.86400
3	256 × 188	3.38900	3.39300
4	512 × 376	13.57800	13.52099

Tampak pada Tabel 2 bahwa waktu proses enkripsi dan dekripsi selisihnya tidak jauh berbeda atau relatif sama. Untuk citra dengan ukuran citra (dalam piksel) yang makin besar dibutuhkan waktu proses enkripsi dan dekripsi yang lebih lama. Hal itu dikarenakan, proses enkripsi dan dekripsi dilakukan secara *stream cipher* yakni perubahan untuk setiap piksel dengan masing-masing *key stream*-nya, sehingga membutuhkan waktu proses yang lebih lama.

Analisis Sensitivitas Kunci

Pada proses pengujian yang dilakukan dalam hal ini menggunakan nilai dari kuncinya adalah selalu sama untuk tiap data uji citra digital. Untuk proses dekripsinya akan diuji cobakan dengan nilai kunci yang berbeda-beda (hanya pada satu parameter kunci saja yakni pada parameter $x_0^{(1)}$). Hal tersebut dilakukan untuk menilai tingkat sensitivitas nilai kunci. Adapun hasilnya disajikan pada Gambar 1.

Gambar 1: Hasil Uji Coba Sensitivitas Nilai Kunci, (a) citra asli, (b) citra hasil enkripsi dengan $x_0^{(1)} = 0.1$ (c) citra hasil dekripsi dengan $x_0^{(1)} = 0.1$, (d) citra hasil dekripsi dengan $x_0^{(1)} = 0.1 + 10^{-20}$, (e) citra hasil dekripsi dengan $x_0^{(1)} = 0.1 + 10^{-21}$)

Terlihat pada Gambar 1, bahwa usaha dekripsi dengan menggunakan kunci yang selisih nilai x_0-nya sebesar 10^{-20} tidak berhasil mendapatkan citra asli (Gambar 1 (d)). Hal ini dikarenakan sifat sensitif terhadap nilai awal dari *logistic map*. Nilai dengan $x_0^{(1)} = 0.1$ dan $x_0^{(1)} = 0.1 + 10^{-20}$ masih dianggap nilai yang berbeda oleh algoritma ini. Sedangkan pada Gambar 1 (e), saat selisihnya mencapai 10^{-21}, usaha dekripsi berhasil mendapatkan informasi citra aslinya. Hal itu menunjukkan bahwa dua bilangan yaitu $x_0^{(1)} = 0.1$dan $x_0^{(1)} = 0.1 + 10^{-21}$ dianggap bilangan yang sama yakni 0.1. Sehingga didapatkan sensitivitas kunci dari algoritma ini adalah sampai 10^{-20}. Dengan demikian akan sangat sulit mendapatkan informasi citra asli melalui serangan *brute force* karena algoritma ini sangat sensitif terhadap perubahan nilai kunci (nilai awal).

Ukuran Ruang Kunci

Kunci yang digunakan pada satu *logistic map* adalah x_0 dan λ, dengan x_0 dan λ adalah bilangan real. Jika digunakan level presisi yang lebih tinggi, misal 64-bit *double precision* maka dari standar IEEE level presisinya akan mencapai 10^{-15}, sehingga banyaknya kemungkinan kunci untuk satu fungsi *logistic map* adalah $10^{15} \times 10^{15} = 10^{30}$. Karena digunakan tiga fungsi logistic map maka total kemungkinan banyaknya kunci adalah $10^{30} \times 10^{30} \times 10^{30} = 10^{90}$. Dengan demikian jika dilakukan usaha untuk mencoba semua kemungkinan yang ada berdasarkan ukuran ruang kunci tersebut maka probabilitas untuk menemukan satu kunci yang cocok adalah sangat kecil sekali yakni mencapai 10^{-90}.

Penutup

Penggunaan multi logistic map dalam algoritma enkripsi citra digital dapat dilakukan dengan baik, berdasarkan kinerja yang dihasilkan sebagai berikut :

- Rata-rata waktu proses enkripsi dan dekripsi relatif sama untuk tiap-tiap citra digital.
- Rata-rata waktu proses enkripsi dan dekripsi citra digital berbanding lurus dengan ukuran citranya (dalam piksel).
- Algoritma enkripsi memiliki ruang kunci sebesar 10^{90}dan sensitivitas kunci (nilai awal) yang mencapai 10^{-20}, sehingga algoritma ini sangat sulit dipecahkan dengan *brute force attack*.

Daftar Pustaka

[1] Stallings, William., (2011), Cryptography and Network Security : Principles and Practice, 5th edition, Pearson Education, Inc., Publishing as Prentice Hall., New Jersey.

[2] Pareek, N.K., Patidar, V., Sud, K.K. (2006). Image encryption using chaotic logistic map. Journal of Image and Vision Computing, 24, 926-934.

[3] Patidar, V., Pareek, N.K., Sud, K.K. (2009). A new subtitution-diffusion based image cipher using chaotic standard and logistic maps. Journal of Commun Nonlinear Sci Numer Simulat, 14, 3056-3075.

[4] Kocarev, L and Lian, S. (2011), Chaos-Based Cryptography : Theory, Algorithm and Applications, Springer-Verlag, Berlin.

[5] Zhang, W., Wong, K., Yu, H., Zhu, Z. (2013). An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. Journal of Commun Nonlinear Sci Numer Simulat, 18, 2066-2080.

[6] Ye, Ruisong and Zhao, Haiying., (2012), An Efficient Chaos-based Image Encryption Scheme using Affine Modular Maps, International Journal Computer Network and Information Security, Vol. 7, pp. 41-50.

[7] Ansari, S., Gupta, N and Agrawal, S., (2012), An Image Encryption Approach Using Chaotic Map in Frequency Domain, International Journal of Emerging Technology and Advanced Engineering, Vol. 2, Issue 8, pp. 287 – 291.

[8] Liu, S, Sun, J and Xu, Z., (2009), An Improved Image Encryption Algorithm based on Chaotic System, Journal of Computer, Academy Publisher,Vol. 4, No. 11, pp.1091-1100.

[9] Abu Zaid, Osama M., El-Fishawy, Nawal A., Nigm, E. M., (2013). Cryptosystem Algorithm Based on Chaotic System for Encrypting Colored Image, International Journal of Computer Science Issues, Vol. 10, Issue 4, July, No 2, pp. 215-224.

[10] Gao, H., Zhang, Y., Liang, S., Li, D. (2006). A new chaotic algorithm for image encryption. Journal of Chaos, Solutons and Fractals , 29, 393-399.

[11] Suryadi MT, Eva Nurpeti, Dhian Widya., (2014), Performance of Chaos-Based Encryption Algorithm for Digital Image. TELKOMNIKA Indonesian Journal of Electrical Engineering. 12(3): 675-682.

[12] Eva, N., Suryadi MT, (2014). Chaos Based Encryption Algorithm for Digital Image, Proceedings IndoMS International Conference on Mathematics and its Applications, pp.169-177.

[13] Suryadi MT, Dhian Widya, (2014). Aplikasi Algoritma Enkripsi Citra Digital Berbasis Chaos Menggunakan Three Logistic Map., Prosiding Seminar Nasional Matematika, Statistika, Pendidikan Matematika dan Komputasi, Vol. 2/No. 1, pp. 344-351.

[14] Munir, Rinaldi., (2011), Enkripsi Selektif Citra Digital dengan Stream Cipher Berbasiskan pada Fungsi Chaotik Logistic map, Prosiding Seminar Nasional dan Ekspo Teknik Elektro, pp. 7 – 12.

[15] Munir, Rinaldi., (2012). Algoritma Enkripsi Selektif Citra Digital Dalam Ranah Frekuensi Berbasis Permutasi Chaos, Jurnal Rekayasa Elektrika, Vol. 10, No. 2, pp. 69-75.

[16] Zhang, Tong., Zhou, Yicong., and Chen, C.L. Philip, (2012), A New Combined Chaotic System for Image Encryption, International Conference on Computer Science and Automation Engineering (CSAE), IEEE. Vol. 2, DOI: 10.1109, pp. 331-335.

[17] Alvarez, Gonzalo., Li, Shujun., (2006)., Some Basic Cryptography Requirements Chaos-Base Cryptosystems, International Journal of Bifurcation and Chaos, Vol. 16, No. 8, pp. 2129-2151.