INTISARI

Analisis Sistem *Robust Chaos* untuk Pembangkitan Kunci Enkripsi Citra

Oleh

AKHMAD SULTONI

23/528781/PPA/06688

Peta logistik merupakan salah satu contoh sistem dinamik waktu diskrit yang menampilkan beragam perilaku pada interval parameter $[0, 4]$, mulai dari keadaan stabil, periodik, hingga bersifat *chaos*. Sifat *chaos* pada peta logistik muncul ketika parameter berada pada kisaran lebih dari $3,65$ hingga 4. Namun, pada rentang *chaos* tersebut masih terdapat jendela-jendela periodik, sehingga peta logistik kurang andal untuk aplikasi yang membutuhkan keacakan tinggi dan konsisten, khususnya di bidang keamanan. Untuk mengatasi keterbatasan ini, penelitian ini mengusulkan modifikasi peta logistik melalui transformasi miring sehingga diperoleh peta logistik miring yang memiliki sifat *robust chaos*. Secara teoritis, sifat *robust chaos* dianalisis menggunakan sebuah teorema pada peta s-unimodal dengan syarat tertentu yang menjamin kemunculan *robust chaos*, dan diperkuat dengan kajian berdasarkan definisi *chaos* Devaney. Secara numerik, perilaku *chaos* pada peta logistik miring divisualisasikan melalui diagram bifurkasi dan eksponen Lyapunov terhadap variasi parameter, yang menunjukkan pola dinamik acak dengan nilai eksponen Lyapunov positif. Selanjutnya, peta logistik miring digunakan untuk membangkitkan kunci enkripsi citra melalui PRNG. Hasil pengujian statistik menggunakan NIST *test* menunjukkan bahwa deret PRNG yang dihasilkan lulus keseluruhan 16 uji dan memenuhi kriteria keacakan. Skema enkripsi citra yang dibangun menghasilkan *ciphertext* dengan tingkat keacakan dan sensitivitas kunci yang tinggi, yang dibuktikan secara kuantitatif melalui nilai NPCR yang melebihi $99,6\%$ dan UACI yang melampaui $33,5\%$. Selain itu, skema ini menunjukkan ketahanan terhadap serangan alterasi yang mana kerusakan citra hingga 40%, hasil dekripsi masih dapat dikenali secara visual. Ruang kunci yang dihasilkan mencapai sekitar $2^{212,6}$, sehingga dapat dikategorikan cukup besar untuk mengantisipasi serangan *brute force*. Dari sisi efisiensi, waktu proses enkripsi untuk citra berukuran 256×256 berada di bawah satu detik, yang mengindikasikan bahwa peta logistik miring memiliki potensi yang baik untuk diterapkan dalam sistem keamanan citra digital.

Kata kunci: peta logistik miring, *robust chaos*, enkripsi citra.

ABSTRACT

Robust Chaos System Analysis for Image Encryption Key Generation

By

AKHMAD SULTONI

23/528781/PPA/06688

The logistic map is an example of a discrete-time dynamical system that exhibits various behaviors over the parameter interval $[0, 4]$, ranging from stable states, periodicity, to chaos. The chaotic behavior in the logistic map arises when the parameter is in the range from 3.65 to 4. However, within this chaotic range, periodic windows still exist, making the logistic map less reliable for applications that require high and consistent randomness, particularly in the field of security. To overcome this limitation, this study proposes a modification of the logistic map through a skew transformation, resulting in a skew logistic map with robust chaotic properties. Theoretically, the robust chaotic behavior is analyzed using a theorem on s-unimodal maps with certain conditions that guarantee the emergence of robust chaos, reinforced by a study based on Devaney's definition of chaos. Numerically, the chaotic behavior of the skew logistic map is visualized through bifurcation diagrams and Lyapunov exponents as the parameter varies, showing random dynamic patterns with positive Lyapunov exponents. Furthermore, the skew logistic map is used to generate image encryption keys through a PRNG. Statistical testing using the NIST test suite shows that the PRNG sequence generated passes all 16 tests and meets the randomness criteria. The image encryption scheme produced results in ciphertexts with high levels of randomness and key sensitivity, quantitatively proven by an NPCR value exceeding 99.6% and an UACI value exceeding 33.5%. Additionally, this scheme demonstrates resilience to alteration attacks, as image degradation of up to 40% still allows for visual recognition after decryption. The key space generated is approximately $2^{212.6}$, which is sufficiently large to withstand brute force attacks. In terms of efficiency, the encryption process for a 256×256 image takes less than one second, indicating that the skew logistic map holds great potential for application in digital image security systems.
Keywords: Skew logistic map, robust chaos, image encryption.