Analisis Komposisi Gauss Map dengan Circle Map dan Implementasinya untuk Enkripsi Data Citra = An Analysis on the Composition of the Gauss Map and the Circle Map and its Implementation for Image Data Encryption

Luqman Nuradi Prawadika, author

Abstrak

Sistem dinamik chaotic dikenal sangat bermanfaat untuk kriptografi data citra digital, karena memiliki beberapa sifat dan perilaku penting, seperti sensitivitas tinggi terhadap keadaan awal, ergodisitas tinggi, dan juga perilaku acak dan aperiodik. Dalam tesis ini, sebuah analisis dilakukan untuk menguji apakah peta chaotic Gauss Map dan Circle Map dapat dikomposisikan untuk menghasilkan sebuah peta chaotic baru yang layak untuk diimplementasikan pada kriptosistem citra digital. Untuk menguji kelayakan ini, Lyapunov Exponents dan diagram bifurkasi dari Gauss Map, Circle Map, dan peta hasil komposisi keduanya dianalisis. Setelah peta chaotic hasil komposisi terbaik diperoleh, peta tersebut diuji kualitas keacakannya sebagai pembangun barisan bilangan pseudorandom menggunakan Uji NIST. Kemudian, sebuah kriptosistem citra digital berbasis One-Time Pad yang mengimplementasikan peta chaotic hasil komposisi tersebut sebagai generator keystream dikonstruksi, yang diujikan pada sepuluh citra digital agar kinerjanya dapat diukur. Peta chaotic yang dihasilkan dari komposisi tersebut memiliki diagram bifurkasi yang himpunan nilai limitnya padat pada domainnya, memiliki nilai-nilai Lyapunov Exponents yang sangat positif, dan hampir lulus seluruh Uji NIST secara sempurna. Kriptosistem yang mengimplementasikan peta chaotic tersebut juga secara sempurna lulus uji-uji sensitivitas, uji ruang kunci, uji korelasi, uji entropi, dan hampir secara sempurna lulus uji histogram.

.....Chaotic dynamical systems are known to be very beneficial for digital image cryptography due to its important properties and behaviors, such as extreme sensitivity to initial conditions, high ergodicity, and its random and aperiodic behaviors. In this thesis, an analysis is conducted to test whether the chaotic Gauss Map and Circle Map can be combined to generate a new chaotic map suitable for digital image cryptosystem implementations. To test this suitability, the Lyapunov Exponents and the bifurcation diagrams of Gauss Map, Circle Map, and their combined map are analyzed. Once the best combined map is obtained, its randomness quality as a pseudorandom number generator (PRNG) is tested using the NIST Test. Then, a digital image cryptosystem based on the One-Time Pad scheme implementing the combined chaotic map as the keystream generator is constructed, which is tested on ten digital images to have its performance measured. The resulting chaotic map from the combination has bifurcation diagrams with dense limit sets within its domain, has very positive Lyapunov Exponents, and almost perfectly passes the entire NIST Test. The cryptosystem implementing the chaotic map also perfectly passes the sensitivity tests, the keyspace test, the correlation test, the entropy test, and almost perfectly passes the histogram