

Kinerja algoritma enkripsi citra digital berbasis chaos = Performance of chaos based encryption algorithm for digital image

Eva Nurpeti, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20368020&lokasi=lokal>

Abstrak

Penyajian informasi secara digital menjadikannya sangat rentan terhadap penyalahgunaannya. Citra digital adalah 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 berbasis chaos yang dapat meningkatkan daya tahan terhadap brute force attack dan known plaintext attack. Algoritma enkripsi tersebut menggunakan logistic map sebagai pembangkit bilangan acak untuk key stream. Diperoleh dari hasil pengujian bahwa ruang kuncinya sebesar 1030, sensitivitas kuncinya 1016, key stream yang dihasilkan terbukti acak, dan distribusi nilai pixel-pixel dari citra terenkripsinya adalah uniform. Sehingga menjadikan algoritma ini sangat sulit dipecahkan oleh brute force attack dan known plaintext attack.

.....

Presentation of information in digital form is highly vulnerable against information abusing. Digital image is one of digital information which is frequently becomes a target of crime. Therefore, reliable, secure, and fast security technique are required in digital image information. In this study, chaos-based encryption algorithm for digital image is built to improve endurance from brute force and known plaintext attack. The algorithm using logistic map as a random number generator for key stream. According to test and analysis, this algorithm has key space of 1030, key sensitivity up to 1016, the key stream is proved random, and the distribution of pixels value from encrypted image is proved uniform. So, it can be concluded that, the algorithm is very difficult to be cracked by brute force attack and also known plaintext attack.