Analisis kinerja new modified map pada enkripsi citra digital = Performance analysis of new modified map for digital image encryption

Maria Yus Trinity Irsan, author

Abstrak

ABSTRAK
Perlindungan terhadap data digital, yang bersifat sangat rahasia, menjadi sangat penting guna menghindari manipulasi dan perubahan data. Data digital dapat berbentuk teks, citra, dan sebagainya. Pembahasan dalam tesis ini terfokus pada proteksi data dan informasi yang berbentuk citra digital. Proteksi yang diberikan adalah dalam bentuk enkripsi citra digital. Proses enkripsi ini menggunakan new map, ( ) ( ), yang merupakan modifikasi dari logistic map. Selanjutnya, new map tersebut dinamakan MS map. Tesis ini menunjukkan tentang: bagaimana hasil enkripsi citra digital dengan menggunakan MS map dan kinerjanya ditinjau dari segi rata-rata waktu proses enkripsi/dekripsi; keacakan barisan key stream dengan uji NIST, analisis histogram, dan uji goodness of fit; dan tingkat sensitivitas nilai awal, parameter, dan ruang kunci.

Hasilnya menunjukkan bahwa rata-rata waktu proses enkripsi relatif sama dengan rata-rata waktu proses dekripsinya dan lamanya waktu proses bergantung pada jenis dan ukuran citra. Ciphertext (citra terenkripsi) berdistribusi seragam karena beberapa hal, yaitu: lulus uji goodness of fit dan histogramnya berbentuk flat; key stream yang dibangkitkan lulus frequency (monobit) test, frequency within a block test, runs test, dan test for the longest run of ones in a block, yang berarti key stream merupakan barisan yang acak; dan tingkat sensitivitas nilai awal mencapai , parameter dan mencapai , dan ruang kunci mencapai . Jadi, algoritma enkripsi yang dikembangkan dengan menggunakan MS map lebih tahan terhadap brute-force attack dan known plaintext attack.
<hr><i>ABSTRACT
Protection to classified digital data becomes so important in avoiding data manipulation and alteration. Digital data may take form as texts, images, et cetera. The focus of this thesis is in data and information protection of digital images form. Protections that are given in this thesis are in the form of digital image encryption. The encryption process uses a new map, ( ) ( ), which is the modification of logistic map. The new map is called MS map.

This thesis will show: the results of digital image encryption using MS map and how the performance is regarding the average time needed for encryption/decryption process; randomness of key stream sequence with NIST test, histogram analysis and goodness of fit test, initial value and parameter sensitivity level, and key space. The results show that the average encryption process time equals the average decryption process time and it depends to types and sizes of the image. Ciphertext (encrypted image) uniformly distributed since: it passes the goodness of fit and also the histogram is flat; key stream, that are generated, passes frequency (monobit) test, frequency within a block test, runs test, and test for the longest run of ones in a block, which means key stream is a random sequence; and initial value sensitivity reaches , parameter dan reach , and key space reaches . So, that encryption algorithm generated by MS map is more resistant to

brute-force attack and known plaintext attack.</i>