

Pengamanan audio digital dengan skema konfusi dan difusi menggunakan double-scroll chaotic function = Digital audio protection with confusion and diffusion scheme using double scroll chaotic function

Muhammad Boyke, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20445448&lokasi=lokal>

Abstrak

Manusia sangat dimanjakan dengan pesatnya perkembangan teknologi, data atau informasi yang disajikan telah berbentuk data digital sehingga semua informasi dapat disimpan dan dikirim dengan sangat mudah. Namun, masalah keamanan dan kerahasiaan data merupakan sesuatu yang sangat vital pada era digital ini, terutama pada data berbentuk audio, audio digital butuh penanganan khusus karena memiliki karakteristik data berkapasitas besar dan tingkat redundansi yang tinggi. Salah satu teknik mengamankan data adalah dengan kriptografi berbasis fungsi chaos. Teknik ini dipercaya dapat mengamankan data karena fungsi chaos memiliki perilaku acak dan sensitif terhadap nilai dengan perubahan sekecil apapun, adapun fungsi chaos double-scroll yang digunakan pada skripsi ini akan dioperasikan dengan fungsi transformasi non-linear untuk mengubah gelombang pada data audio, sehingga pesan pada data audio akan terjamin keamanannya. Pada skripsi ini akan dibahas bagaimana mengamankan data berbentuk audio menggunakan fungsi chaos double-scroll dengan skema konfusi dan difusi, adapun ruang kunci yang dihasilkan oleh algoritma ini mencapai 1.04×10^{124} dengan sensitivitas kunci mencapai 10-14 sehingga membuat algoritma ini sulit untuk dipecahkan dengan bruteforce attack. Dengan nilai koefisien korelasi antara audio terenkripsi dan audio asli memiliki nilai -0.000048 mengindikasikan rendahnya hubungan ataupun kemiripan antara keduanya. Hasil uji analisis histogram dan uji goodness of fit memberikan hasil audio terenkripsi berdistribusi uniform sehingga algoritma ini memiliki ketahanan yang baik dari statistical attack. Dilakukan pula uji Peak Signal-to-Noise Ratio pada audio terenkripsi dengan nilai 4.6548 merupakan nilai yang amat kecil mengindikasikan audio terenkripsi terdengar sangat bising. Sehingga, kerahasiaan informasi yang terdapat dalam audio tetap terjaga.

<hr>

People very spoiled with the rapid development of technology, all information have been digitized so its can be stored and shipped easily. However, the issue of security and confidentiality of data are something very vital in this era, especially the data in audio form. Digital audio need special treatment because it has characteristics of large capacity data and a high level of redundancy. One technique to secure the data is chaos based cryptography. This technique can be trusted to secure the data, due to a chaos function has random behavior, and are very sensitive to the slightest change on initial condition. This paper uses double scroll chaotic function with confusion and diffusion schemes and it will be operated with non linear transformation function to change the signal of audio data so that it can guarantee its security. This paper will discuss how to secure data in audio form using double scroll chaotic function with confusion and diffusion scheme. The algorithm owns large key space 1.04×10^{124} to make brute force attack impossible. The corelation coefficient test give value of 0.000048 indicates less resemblance between them. Histogram analysis and goodness of fit test shows that the encrypted audio has uniform distribution and thus showed that the algorithm invulnerable to statistical attack. The peak signal to noise ratio test result give value of

4.6548, which means encrypted audio sound very noisy. Thus, the confidentiality of the information contained in audio is maintained.