

Pengamanan suara digital dengan menggunakan normalized complex quadratic map = Digital audio security using normalized complex quadratic map

Tjandra Satria Gunawan, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20458930&lokasi=lokal>

Abstrak

ABSTRAK

Pada era digital saat ini, penggunaan teknologi sudah menglobal, bertukar data merupakan hal yang biasa dan mudah dilakukan sehingga data rentan terhadap penyerangan atau manipulasi dari pihak yang tidak bertanggung jawab. Salah satu jenis data yang rentan terhadap penyerangan ini adalah suara digital. Sehingga, diperlukan suatu metode pengamanan data yang kuat dan cepat. Salah satu metode pengamanan yang memenuhi semua kriteria tersebut adalah pengamanan data menggunakan fungsi chaos. Fungsi chaos yang digunakan pada penelitian ini adalah fungsi Normalized Complex Quadratic Map NCQM . Fungsi NCQM memiliki kelebihan yaitu dijamin bersifat chaos ketika parameter fungsinya memiliki nilai absolut yang lebih kecil dari satu. Barisan kunci yang dibangkitkan dengan fungsi NCQM lolos semua 15 uji NIST, hal ini berarti pembangkitan barisan kunci key stream dari fungsi NCQM ini terbukti bersifat acak random . Selain itu, hasil sampel-sampel dari suara digital yang telah terenkripsi ketika diuji dengan histogram dan uji Goodness of Fit terbukti uniform sehingga pengamanan suara digital dengan metode ini kebal terhadap frequency analysis attack. Ruang kunci yang dihasilkan dari metode ini sangat besar yaitu 9,1 1046 untuk kemungkinan kunci pada fungsi NCQM tunggal, dan 3,8 10109 untuk NCQM ganda , sehingga metode ini juga kebal terhadap brute force attack.

ABSTRAK

In this digital era, technology usage has been globalized in which data exchange is common and easy to do, it is vulnerable to be attacked and manipulated from unauthorized parties. One data type that is vulnerable to attack is digital audio. So, we need data security method that secure and fast. One of the methods that match all of those criteria is data security using "chaos" function. "Chaos" function that is used in this research is Normalized Complex Quadratic Map NCQM . NCQM function has advantages that are guaranteed to be "chaos" when the function parameter has absolute value less than one. The key stream that is generated using this NCQM functions passed all 15 NIST tests, this means that the key stream generated by NCQM proved to be random. In addition, samples of encrypted digital sound when tested using histogram and Goodness of Fit test are proved to be uniform so this digital audio security using this method is immune to frequency analysis attack. The key space that is generated from this method is very huge approximately 9,1 1046 possible keys for single NCQM function, and approximately 3,8 10109 for multiple NCQM function , therefore this method is also immune against brute force attack.