Abstract

In this paper an algorithm for speech encryption based on three dimension chaotic maps is proposed. The proposed algorithm consists of three main units: generation of keys, samples substitution and samples permutation process. In order to maximize the benefits of the substitution process, it is performed in two stages with cipher feedback, for the system. Moreover bit-level permutation for sample is introduced as substitution mechanism in the permutation stage. The Lorenz and Rossler chaotic system are employed as generation of keystream used for substitution and permutation process respectively. From the experimental results, it is concluded that the proposed algorithm has the advantages of very low residual intelligibility, key sensitivity and high quality recovered signal, and moreover the proposed algorithm can resist known-plaintext attacks and supports large key space make brute-force attacks infeasible.


Index Terms

Computer Science  Signal Processing
Keywords

Speech encryption, Residual intelligibility, Lorenz system, Rossler system, Permutation, Substitution, Residual intelligibility.