Abstract

In this paper a new speech encryption system is presented. It is based on permutation and substitution of speech samples using secret keys in time and transform domains. The system is with multilevel to increase the security and to present an encrypted signal with low residual intelligibility. The logistic map is employed in keys generation to generate permutation and mask keys to be used in the permutation and substitution process. In order to maximize the benefits of the permutation process for the system, Arnold cat map is applied to permute the samples in the last level of encryption system. Simulations results are presented in the paper indicate that the encryption system provides encryption speech signal of low residual intelligibility, key sensitivity and high quality recovered signal. Total key space for the proposed encryption system is \(2^{348}\), which is large enough to protect the encryption signal against brute-force attack.

References

- Sadkhan Sattar B. and Abbas Nidaa A., "Performance Evaluation of Speech Scrambling Methods Based on Statistical Approach"; ATTI DELLA "Fonazione"
Giorgio Ronchi; Anno Lxvi, No. 5 PP. 601-6014 (2011).

Index Terms

Computer Science

Security

Keywords
A Speech Encryption based on Chaotic Maps

Speech encryption  Logistic map  Arnold cat map  Permutation  Substitution
Residual intelligibility.