World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:9, No:11, 2015

An Algorithm Based on the Nonlinear Filter Generator for Speech Encryption

Authors : A. Belmeguenai, K. Mansouri, R. Djemili

Abstract : This work present a new algorithm based on the nonlinear filter generator for speech encryption and decryption. The proposed algorithm consists on the use a linear feedback shift register (LFSR) whose polynomial is primitive and nonlinear Boolean function. The purpose of this system is to construct Keystream with good statistical properties, but also easily computable on a machine with limited capacity calculated. This proposed speech encryption scheme is very simple, highly efficient, and fast to implement the speech encryption and decryption. We conclude the paper by showing that this system can resist certain known attacks.

Keywords : nonlinear filter generator, stream ciphers, speech encryption, security analysis
Conference Title : ICSIP 2015 : International Conference on Signal and Information Processing
Conference Location : Paris, France
Conference Dates : November 19-20, 2015