A semi-one time pad using blind source separation for speech encryption

許隆結,Horng-Shing Chiou,Wei Ching Chen
Mechanical Engineering
Engineering
ljsheu@chu.edu.tw

Abstract

We propose a new perspective on speech communication using blind source separation. The original speech is mixed with key signals which consist of the mixing matrix, chaotic signals and a random noise. However, parts of the keys (the mixing matrix and the random noise) are not necessary in decryption. In practice implement, one can encrypt the speech by changing the noise signal every time. Hence, the present scheme obtains the advantages of a One Time Pad encryption while avoiding its drawbacks in key exchange. It is demonstrated that the proposed scheme is immune against traditional attacks.

Keyword：one time pad, blind source separation, independent