Abstract

Chaotic behaviour is one of the most complex dynamics that a nonlinear system can exhibit. Because the signals resulting from chaotic systems are broadband, noiselike, difficult to predict, the idea of using chaotic systems for information masking has received much attention since the pioneering work of Carroll and Pecora from 1991.

This thesis is investigating the applications of the chaotic behaviour in the field of cryptography. A theoretical description of the cryptosystems in this field require notions from various domains. Thus, there are combined elements of information theory (information channel and associated sizes) with a series of statistical methods (Smirnov tests, Kolmogorov-Smirnov tests and an original method to verify the statistical independence in the case of continuous random variables which obey Gaussian law or not - the last method can be applied on all types of random variables, even if they obey an unknown type of probability law). Other notions like observability and singularity are used to characterize the topological behaviour of the chaotic systems.

A new enciphering method or an approach between the chaotic behaviour and the new sampling technique are directions which make the contributions of the proposed work very useful.

Comportamentul haotic este unul dintre cele mai complexe tipuri de comportament ale unui sistem neliniar. Deoarece semnalele care rezultă din sistemele haotice sunt de bandă largă, greu de prezis, ideea de a folosi sistemele haotice pentru mascarea informaţiei s-a bucurat de multă atenţie începând de la cercetările făcute de Carroll şi Pecora din 1991.

Această teză işi propune investigarea şi construirea de aplicaţii folosind comportamentul haotic. O descriere teoretică a unui criptosistem necesită abordarea de notiuni din domenii variate. Asfel, sunt combinate instrumente de descriere şi prelucrare a proceselor aleatoare cu teste Smirnov, teste Kolmogorov-Smirnov, analiză Monte Carlo, precum şi cu o metodă originală de verificare a independenţei statistice în cazul variabilelor aleatoare continue care prezintă lege gaussiană sau nu; această metodă poate fi aplicată pentru variabile aleatoare chiar şi de lege de probabilitate necunoscută. Noţiuni precumobservabilitatea şi singularitatea se folosesc pentru caracterizarea sistemelor haotice din punct de veder3e topologic.

O nouă metodă de criptare sau folosirea comportamentului haotic în implementarea unei noi thenici de eşantionare a semnalelor sunt direcţii care arată interesul contribu- ţiilor acestei teze.