ISSN 0735-2727, Radioelectronics and Communications Systems, 2010, Vol. 53, No. 5, pp. 261–264. © Allerton Press, Inc., 2010.
Original Russian Text © P.Yu. Kostenko, S.N. Symonenko, A.N. Barsukov, K.S. Vasiuta, 2010, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2010, Vol. 53, No. 5, pp. 41–45.

Use of BDS Statistic to Estimate Security of a Signal Obtained by Mixing Chaotic Carrier

P. Yu. Kostenko, S. N. Symonenko, A. N. Barsukov, and K. S. Vasiuta

Kharkiv Air Force University, Kharkiv, Ukraine

Received in final form February 19, 2010

Abstract—Efficiency of using the method of mixing a chaotic carrier to provide signal security in information transmission systems with use of BDS statistic is studied in this work. By means of statistical modeling for a specific example the increase in security by more than four times is demonstrated.

DOI: 10.3103/S0735272710050055

One of the modern approaches to providing security of information transmission systems (ITS) is based on using a chaotic carrier to operate “beneath noise” (random process) [1, 2]. It is assumed that security is provided due to its visual similarity to noise, absence of obvious order (regularity) and low probability of recognizing chaotic and random processes within correlation and spectral analysis. Such arguments in favor of providing ITS security by means of chaotic carrier do not account for one significant thing. There is an arsenal of methods and means, developed in the theory of chaotic dynamic systems, which may be involved to ensure more complete accounting for limitations and possibilities of ITS, which use achievements of chaotic dynamics. One of such most important methods allows obtaining non-trivial information on a chaotic process (sequence) by analyzing its trajectory in the phase (pseudo-phase) space. Evolution of chaotic process represented in the phase space demonstrates regular (probably self-similar) behavior. The mentioned property is also inherent to determined processes. However in case of random processes with independent and identical distributed (IID) and with dependent values (for example, colored noise) a set of points in the phase space is unstructured and practically impossible to combine in “trajectory”. As an example, the phase portraits of a random sequence $\Xi = \{\xi_m\}_{m=0}^{M-1}$ with uniform distribution within (0, 1) and of a chaotic process formed by integration of the 3rd-order Chebyshev polynomial $T_d(x)$ with $g(x) = T_3(x) = 4x^3 - 3x$ are depicted in Fig. 1.

Dimensionality is one of structuring measures of a process (dependence of its values) in the phase space. Use of this measure allows revealing dependences between process’s values, extracting necessary information on the kind of its generating mapping, and, as a consequence, obtaining more independent estimation of potential security of chaotic carrier. Obviously without accounting for information on the possible structuring of the analyzed process this estimate will be inflated. We should note that security often means an ability to resist measures of radio intelligence [3]: signal detection and determination of its structure using estimation of a number of its parameters. As a security criterion one may use a quantity $p_{\text{sec}} = 1 - p_{\text{i}}$, which is determined by intelligence probability $p_{\text{i}} = p_{\text{det}} p_{\text{str}}$, defined by correct detection probability p_{det} (checking two hypothesis: on the presence of noise (hypothesis H_0) or signal and noise (hypothesis H_1)) and probability of recognizing its structure p_{str}. This work assumes that the problem of revealing the meaning of information is not set. In stenographic information security methods security has a similar meaning, while estimation of its level is accomplished by revealing a number of statistical properties of a digital data stream (without noise factor), which to some degree reflects statistical dependences in data [4].

In the considered case of using a chaotic carrier security is determined with accounting for correct classification probability of the analyzed process: white noise (hypothesis H_0) or chaotic process in absence of noise (hypothesis H_1). Thus, instead of probability p_{det} we determine the probability of correct signal classification p_{cl}. This characteristic is sufficient to determine the lower security boundary, which characterizes the most unfavorable from the point of view of the “beneath noise” operation mode. Presence of noise in the observation of chaotic signal would only increase this boundary.