*Journal of Communications Technology and Electronics, Vol. 50, No. 12, 2005, pp. 1358–1366. Translated from Radiotekhnika i Elektronika, Vol. 50, No. 12, 2005, pp. 1466–1475.*
*Original Russian Text Copyright © 2005 by Loskutov, Rybalko.*
*English Translation Copyright © 2005 by MAIK "Nauka /Interperiodica" (Russia).*

# Applications of Dynamical Systems with External Perturbations for Information Encoding and Hidden Data Transmission

**A. Yu. Loskutov and S. D. Rybalko**

Received October 20, 2002

**Abstract**—A new method for information processing and hidden data transmission is proposed that uses stabilized orbits of the families of dynamical systems for encoding alphabetic characters, which are put in a biunique correspondence with the periods of such orbits. An allowable noise level in the communications channel and the degree of randomness of transmitted signals are analytically estimated. The examples of encoded letter sequences are presented.

## INTRODUCTION

Currently, there is a particular interest in nontraditional methods for information processing (e.g., see [1–11] and references therein). This is due to a rapid recent growth of requirements for information security. Ordinarily, information security is meant as the protection of information against illegal access by unauthorized users [12–14].

A new method of encryption for the protection of information relates to the applications of the modern theory of dynamical systems, which considers chaotic signals as data carriers [3, 6, 8, 9, 11, 15–19]. Recent results obtained in this field substantially extend the range of methods available for data storage and data transmission.

It is known that the behavior of chaotic systems sensitively depends on initial conditions and external perturbations. For a long time, such systems were considered unsuitable for practical applications because of their seemingly unpredictable and uncontrollable performance. However, further investigation demonstrated that such systems not only can be controlled but also can be used for practical applications. In particular, along with the recording–readout of data, chaotic systems proved to be adaptable for the hidden transmission of information. Investigations in this area are mainly based on the two following assumptions.

(i) Certain periodic trajectories can be stabilized by using external perturbations [20–26].

(ii) Under specific conditions, two independent chaotic systems can be synchronized [27–31].

It is known that a dynamical system may be defined either in the form of maps or by differential equations. In the first case, the methods of trajectory stabilization are most frequently used, thus making it possible to construct fairly efficient data transmission systems (see, e.g., [5–8, 15, 18, 19]). The second variant (differential equations) is preferable for the problems concerning synchronization. In this case, analog devices can be constructed (see [27, 28, 32–35, and references therein]).

In this study, we propose an algorithm based on stabilization of periodic trajectories in one-dimensional (1D) maps for the hidden transmission of information. The method of stabilization is based on a known fact [22, 23, 26] that, for considerably general families of 1D maps, orbits of a certain period can be stabilized by applying external periodic perturbations. The stable orbits of a perturbed map are used to encode information. The perturbations are transmitted as a useful signal, and the mapping function presents the key for decrypting the received message. In this study, we propose an encoding algorithm that can be implemented in practice and can describe the results of applying this algorithm to a family of quadratic maps.

## 1. STABILIZATION OF PREDETERMINED ORBITS BY MEANS OF PARAMETRIC PERTURBATIONS

Let us consider the mapping of a certain region $M$ from $\mathbf{R}^j$ onto itself:

$$T_a : \mathbf{x} \mapsto \mathbf{f}(\mathbf{x}, a), \tag{1}$$

where $a$ is a parameter from the set of admissible values $A \subset \mathbf{R}$, $\mathbf{x} = \{x_1, \dots, x_j\}$, and $\mathbf{f} = \{f_1, \dots, f_j\}$.

Let us introduce the concept of parametric perturbation. Assume that the mapping is specified with respect to a parameter in such a way that its value is defined at every instant; i.e., $G : A \longrightarrow A$. Then, the perturbed map has the form

$$\mathbf{T}_a : \begin{cases} \mathbf{x} \mapsto \mathbf{f}(\mathbf{x}, a) \\ a \mapsto g(a). \end{cases} \tag{2}$$

Perturbation will be referred to as *periodic* with period $\tau$ if function $g(a)$ is defined only at points $a_1, \ldots, a_\tau$ in the following way: $a_{i+1} = g(a_i)$, $i = 1, \ldots, \tau - 1$, and $a_1 = g(a_\tau)$. In other words, perturbation is specified by the successive substitution of $\tau$ parameters into map (1). In this case, the totality of perturbations with period $\tau$ can be put in correspondence with the set $\mathbf{A} = \{\hat{a} \in \underbrace{A \otimes A \otimes \ldots \otimes A}_{\tau\ \text{times}} : \hat{a} = (a_1, \ldots, a_\tau), a_i \neq a_j, 1 \le i, j \le \tau, i \neq j, a_1, \ldots, a_\tau \in A\}$, $\mathbf{A} \subset \mathbf{R}^\tau$.

Having introduced the periodic perturbation with period $\tau$ for map (1), we obtain for perturbed map (2):

$$\mathbf{T} = \begin{cases} T_{a_1} : \mathbf{x} \mapsto \mathbf{f}(\mathbf{x}, a_1) \equiv \mathbf{f}_1 \\ T_{a_2} : \mathbf{x} \mapsto \mathbf{f}(\mathbf{x}, a_2) \equiv \mathbf{f}_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ T_{a_\tau} : \mathbf{x} \mapsto \mathbf{f}(\mathbf{x}, a_\tau) \equiv \mathbf{f}_\tau. \end{cases} \tag{3}$$

Let us consider $\tau$ functions of the form

$$\begin{aligned} \mathbf{F}_1 &= \mathbf{f}_\tau(\mathbf{f}_{\tau-1}(\ldots\mathbf{f}_2(\mathbf{f}_1(\mathbf{x}))\ldots)), \\ \mathbf{F}_2 &= \mathbf{f}_1(\mathbf{f}_\tau(\mathbf{f}_{\tau-1}(\ldots\mathbf{f}_3(\mathbf{f}_2(\mathbf{x}))\ldots))), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \mathbf{F}_\tau &= \mathbf{f}_{\tau-1}(\mathbf{f}_{\tau-2}(\ldots\mathbf{f}_1(\mathbf{f}_\tau(\mathbf{x}))\ldots)), \end{aligned} \tag{4}$$

where $\mathbf{x} = \{x_1, \ldots, x_j\}$, $\mathbf{f}_i = \{f_i^{(1)}, \ldots, f_i^{(j)}\}$, and $\mathbf{F}_i = \{F_i^{(1)}, \ldots, F_i^{(j)}\}$ are $j$-component functions, $i = 1, 2, \ldots, \tau$. In terms of these functions, perturbed map (2) appears as

$$\begin{aligned} &T_1 : \mathbf{x} \mapsto \mathbf{F}_1(\mathbf{x}, a_1, \ldots, a_\tau), \\ &T_2 : \mathbf{x} \mapsto \mathbf{F}_2(\mathbf{x}, a_1, \ldots, a_\tau), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &T_\tau : \mathbf{x} \mapsto \mathbf{F}_\tau(\mathbf{x}, a_1, \ldots, a_\tau), \end{aligned} \tag{5}$$

with the initial conditions $\mathbf{x}_1 = \mathbf{f}_1(\mathbf{x}_0)$ and $\mathbf{x}_2 = \mathbf{f}_2(\mathbf{x}_1)$, …, $\mathbf{x}_{\tau-1} = \mathbf{f}_{\tau-1}(\mathbf{x}_{\tau-2})$.

According to [26, 36], the maps constructed above have the following important properties.

Let us assume that transformation $T_k$, $1 \le k \le \tau$, has a orbit with period $t$ and functions $\mathbf{f}_k(\mathbf{x})$ are continuous. Under this assumption, map $T_p$, $p = k + 1\ (\mathrm{mod}\,\tau)$, also has a orbit with period $t$. Moreover, if the orbit of map $T_k$ is stable, then, the periodic orbit of map $T_p$ is stable as well and, if $\mathbf{f}_k$ is a geomorphism, maps $T_k$ and $T_p$ are topologically equivalent.

Indeed, the existence of the orbit entails that $\mathbf{F}_k^t(\tilde{\mathbf{x}}) = \tilde{\mathbf{x}}$ and $\mathbf{F}_k^j(\tilde{\mathbf{x}}) \neq \tilde{\mathbf{x}}$, $1 \le j < t$. Consider the relationship that follows directly from the definition of $\mathbf{F}_k$:

$$\mathbf{f}_k(\mathbf{F}_k(\mathbf{x})) = \mathbf{F}_p(\mathbf{f}_k(\mathbf{x})), \quad p = k + 1\ (\mathrm{mod}\tau). \tag{6}$$

It can be seen readily that $\mathbf{f}_k(\boldsymbol{F}_k^n) = \mathbf{F}_p^n(\mathbf{f}_k)$. Therefore, for point $\tilde{\mathbf{x}}$ and $n = t$, we find $\mathbf{F}_p^t(\mathbf{f}_k(\tilde{\mathbf{x}})) = \mathbf{f}_k(\boldsymbol{F}_k^t(\tilde{\mathbf{x}})) = \mathbf{f}_k(\tilde{\mathbf{x}})$. Furthermore, when $1 \le l < t$, we have $\mathbf{F}_p^l(\mathbf{f}_k(\tilde{\mathbf{x}})) \neq \mathbf{f}_k(\tilde{\mathbf{x}})$ because, if it were $\mathbf{F}_p^l(\mathbf{f}_k(\tilde{\mathbf{x}})) = \mathbf{f}_k(\tilde{\mathbf{x}})$, we would arrive at $\mathbf{F}_p^l(\mathbf{f}_k(\tilde{\mathbf{x}})) = \mathbf{f}_k(\mathbf{F}_k^l(\tilde{\mathbf{x}})) = \mathbf{f}_k(\tilde{\mathbf{x}})$. However, by virtue of the uniqueness of functions $\mathbf{f}_i$, $i = 1, \ldots, \tau$, it follows that $\mathbf{f}_{k-1}(\mathbf{f}_{k-2}(\ldots\mathbf{f}_k(\mathbf{F}_k^l(\tilde{\mathbf{x}})))) = \mathbf{f}_{k-1}(\mathbf{f}_{k-2}(\ldots\mathbf{f}_k(\tilde{\mathbf{x}})))$ (see (4)); i.e., $\mathbf{F}_k^{l+1}(\tilde{\mathbf{x}}) = \mathbf{F}_k(\tilde{\mathbf{x}})$. However, this contradicts the above assumption. In other words, point $\mathbf{f}_k(\tilde{\mathbf{x}})$ is periodic with period $t$ for map $T_p$.

If point $\tilde{\mathbf{x}}$ is a stable periodic point of map $T_k$, then there exists such a vicinity $U \ni \tilde{\mathbf{x}}$ that the relationship $\lim\limits_{n \to \infty} \mathbf{F}_k^{tn}(\mathbf{x}) = \tilde{\mathbf{x}}$ holds true for each point $\mathbf{x} \in U$. In view of continuity of functions $\mathbf{f}_k$, this leads to $\lim\limits_{n \to \infty} \mathbf{f}_k(\mathbf{F}_k^{tn}(\mathbf{x})) = \lim\limits_{n \to \infty} \mathbf{F}_p^{tn}(\mathbf{f}_k(\mathbf{x})) = \mathbf{f}_k(\tilde{\mathbf{x}})$. In other words, all points from the vicinity of $\mathbf{f}_k(U)$ tend to point $\mathbf{f}_k(\tilde{\mathbf{x}})$ under map $T_p^t$.

Topological equivalence follows directly from (6) and the definition.

The essence of the above statements is that the investigation of a periodically perturbed map can be substantially simplified. Thus, instead of initial nonautonomous map (2), any one of autonomous maps $T_1$, $T_2$, …, $T_\tau$ defined by relationships (4) and (5) can be considered. Thereby, the dynamical behavior of initial map (2) is completely specified by the totality of maps (5), which act independently of one another and are coupled by only the initial conditions. It follows from this [23, 26, 36] that period $t$ of any orbit of perturbed map (2) is a multiple of perturbation period $\tau$: $t = \tau n$, where $n$ is an integer.

Note that neither the construction of maps $T_1, \ldots, T_\tau$ by formulas (3)–(5) nor the proof of the statements required restrictions on set $A$. In other words, all the results are true for arbitrary set $A$ of allowable values $a$ of dynamical system (1) with $\tau$-periodic perturbation (2).

Let us form a subset $A_{\mathrm{ch}} \subset A$ of the set of parametric values such that map (1) has chaotic behavior if $a \in A_{\mathrm{ch}}$. In a number of studies (see, e.g., [22, 23, 36, 37]), it was analytically substantiated that, at $j = 1$ and $j = 2$, the periodic perturbations may suppress the chaos and stabilize the map orbits. It was also shown that, for certain 1D and 2D chaotic maps, there are such perturbations $\hat{a} = (a_1, a_2, \ldots, a_\tau)$ that perturbed map (2) becomes regular and has a stable orbit with period $t = \tau n$ when $\hat{a} \in \mathbf{A}_{\rm ch}$, $\mathbf{A}_{\rm ch} = \underbrace{A_{\rm ch} \otimes A_{\rm ch} \otimes \ldots \otimes A_{\rm ch}}_{\tau \text{ times}}$ (or $g(a) \in A_{\rm ch}$, see (2)).

This result is proved for a wide class of maps [26, 38]. The property to display periodic dynamics under the action of external perturbations seems to be typical for a fairly wide class of maps.

For practical implementation of encoding and transmission of information by means of perturbed maps, it is required to know how to find such τ-periodic transforms $G : a \mapsto g(a)$ for map (2) that convert it into a map having a stable orbit. Let us restrict the consideration to 1D ($j = 1$) maps. In this case, the theory developed in [22, 36, 37, 39] can be generalized and the method of searching for special perturbations allowing the stabilization of preassigned orbits becomes applicable for practical purposes (see Section 3).

Let map $T_a : x \mapsto f(x, a)$, $x \in M$, $a \in A$ possess the following properties:

(i) There exists a subset $\sigma \subset M$ such that a value $a^* \in A$ that satisfies the equality $f(x_1, a^*) = x_2$ can be found for any $x_1, x_2 \in \sigma$.

(ii) There is a critical point $x_{\rm c} \in \sigma$ such that $\partial f(x, a)/\partial x|_{x = x_{\rm c}} \equiv D_x f(x_{\rm c}, a) = 0$ for all $a \in A$.

In this case, it can be readily shown that, for all $x_2, x_3, \ldots, x_\tau \in \sigma$, there are $x_1$ and $a_1, a_2, \ldots, a_\tau$ such that orbit $(x_1, x_2, \ldots, x_\tau)$ is a stable orbit of perturbed map $\mathbf{T}_a$ for $\hat{a} = (a_1, \ldots, a_\tau)$.

Indeed, let us select arbitrary elements $x_1, x_2, \ldots, x_\tau$. By definition (1), the system of equations

$$\begin{gathered} f(x_1, a_1) = x_2, \\ f(x_2, a_2) = x_3, \ldots, f(x_\tau, a_\tau) = x_1 \end{gathered} \tag{7}$$

for parameters $a_1, a_2, \ldots, a_\tau$ has the solution in the form $\hat{a} = (a_1, a_2, \ldots, a_\tau)$. Therefore, sequence $(x_1, x_2, \ldots, x_\tau) = p$ is the τ-periodic orbit of map $\mathbf{T}_a$ with periodic perturbation $\hat{a} = (a_1, a_2, \ldots, a_\tau)$. To make orbit $p$ stable, it is sufficient to select element $x_1$ near or at critical point $x_{\rm c}$, because $\beta(p) \equiv \prod_{i=1}^{\tau} D_x f(x_i, a_i)$ and $D_x f(x_{\rm c}, a) = 0$ for every $a$. This provides the stability criterion $|\beta(p)| < 1$.

Now, let us estimate the admissible distortions of parameters $(a_1, a_2, \ldots, a_\tau)$ and orbit elements $(x_1, x_2, \ldots, x_\tau)$. Let perturbation $(a_1, a_2, \ldots, a_\tau)$ correspond to stable orbit $(x_{\rm c}, x_2, x_3, \ldots, x_\tau)$. Assume that parameters $a_i$ have slightly changed to become $(a'_1, a'_2, \ldots, a'_\tau) = (a_1 + \Delta a_1, a_2 + \Delta a_2, \ldots, a_\tau + \Delta a_\tau)$, where $|\Delta a_i| \le \delta_a$. Let us find the maximum value of $\delta_a$ at which the perturbed orbit remains stable and study the corresponding orbit distortions, i.e., determine $\Delta x_i$ for $(x'_1, x'_2, \ldots, x'_\tau) = (x_{\rm c} + \Delta x_1, x_2 + \Delta x_2, \ldots, x_\tau + \Delta x_\tau)$. This approach can be formalized as follows.

Let perturbed map $\mathbf{T}_a$ have a stable τ-periodic orbit $p = (x_1, x_2, \ldots, x_\tau)$ for $\hat{a} = (a_1, a_2, \ldots, a_\tau)$. If

$$|\Delta a_i| \le \delta_a = \frac{1}{\tau S_a L S_x^{\tau-1} \sum_{i=1}^{\tau} S_x^i},$$

where $i = 1, 2, \ldots, \tau$, $S_a = \max_{x,a} |D_a f(x, a)|$, $L = \max_{x,a} |D_x^2 f(x, a)|$, and $S_x = \max_{x,a} |D_x f(x, a)|$, then this map has another stable τ-periodic orbit $p' = (x_{\rm c} + \Delta x_1, x_2 + \Delta x_2, \ldots, x_\tau + \Delta x_\tau)$, where $|\Delta x_i| \le \delta_x = 1/LS_x^{\tau-1}$ for $\hat{a}' = (a_1 + \Delta a_1, a_2 + \Delta a_2, \ldots, a_\tau + \Delta a_\tau)$.

In order to substantiate the above estimate, we assume that all parameters $a_i$ are perturbed: $a'_i = a_i + \Delta a_i$. Let us find variation $\Delta x_1 = x'_1 - x_{\rm c}$. Here, element $x'_1$ is a fixed point of map $T_1$ (see (5)); i.e., $x'_1 = F_1(x'_1, a'_1, a'_2, \ldots, a'_\tau)$. This yields $x_{\rm c} + \Delta x_1 = F_1(x_{\rm c}, a_1, a_2, \ldots, a_\tau) + D_x F_1(x_{\rm c}, \hat{a})\Delta x_1 + \sum_{i=1}^{\tau} D_{a_i} F_1(x_{\rm c}, \hat{a})\Delta a_i$. Taking into account the relationships $x_{\rm c} = F_1(x_{\rm c}, \hat{a})$ and $D_x F_1(x_{\rm c}, \hat{a}) = \beta(p) = 0$, we obtain $\Delta x_1 = \sum_{i=1}^{\tau} \prod_{l=i+1}^{\tau} D_x f(x_l, a_l) D_a f(x_i, a_i)\Delta a_i$. Therefore,

$$\begin{aligned} |\Delta x_1| &\le \delta_a \sum_{i=1}^{\tau} \prod_{l=i+1}^{\tau} |D_x f(x_l, a_l)||D_a f(x_i, a_i)| \\ &\le \delta_a \tau S_a \sum_{i=1}^{\tau} S_x^i. \end{aligned} \tag{8}$$

Let us estimate the change of the multiplier of the orbit, $\beta(p') = \prod_{i=1}^{\tau} D_x f(x'_i, a'_i) = \sum_{i=1}^{\tau} D_x^2 f(x_i, a_i) \prod_{\substack{l=1 \\ l \ne i}}^{\tau} D_x f(x_l, a_l)\Delta x_i + \sum_{i=1}^{\tau} D_{ax}^2 f(x_i, a_i) \prod_{\substack{l=1 \\ l \ne i}}^{\tau} D_x f(x_l, a_l)\Delta a_i$. In both sums, only the first terms are nonzero, since $D_x f(x_1, a_1) = D_x f(x_{\rm c}, a_1) = 0$. Therefore, $\beta(p') = [D_x^2 f(x_{\rm c}, a_1)\Delta x_1 + D_{ax}^2 f(x_{\rm c}, a_1)\Delta a_1] \prod_{l=2}^{\tau} D_x f(x_l, a_l)$. However, $D_{ax}^2 f(x_{\rm c}, a_1) = D_a(D_x f(x_{\rm c}, a))|_{a = a_1} = D_a(0) = 0$; therefore, $|\beta(p')| = |\Delta x_1||D_x^2 f(x_{\rm c}, a_1)| \prod_{l=2}^{\tau} |D_x f(x_l, a_l)|$. The orbit remains stable under the condition $|\Delta x_1||D_x^2 f(x_c, a_1)|\prod_{l=2}^{\tau}|D_x f(x_l, a_l)| \le |\Delta x_1| L S_x^{\tau-1} < 1$. Hence, it follows that $|\Delta x_1| \le \delta_x = 1/(LS_x^{\tau-1})$.

Thus, we find that the orbit is stable if perturbation $\Delta x_1$ is less than $\delta_x$. The relation between the maximum possible value of $\Delta x_1$ and $\delta_a$ is given by inequality (8). Finally, the restriction imposed on $\delta_a$ is obtained in the form $\delta_a \tau S_a \sum_{i=1}^{\tau} S_x^i = 1/(LS_x^{\tau-1})$ or

$$\delta_a = \frac{1}{\tau S_a L S_x^{\tau-1} \sum_{i=1}^{\tau} S_x^i}.$$

These results validate the use of chaotic maps for the efficient encoding and hidden transmission of information.

## 2. USING THE STABILIZED ORBITS OF PERTURBED MAPS FOR THE ENCODING AND TRANSMISSION OF INFORMATION

The original method for hidden transmission of information is based on the encoding of alphabetic symbols by the stabilized orbits of chaotic maps and can be implemented in the following manner. Let the period of each orbit stabilized (by selecting the perturbation) be assigned to a certain alphabetic symbol. The encoded symbol is transmitted when the assigned perturbation is sent to a receiver. The decoding procedure consists in applying the transmitted periodic perturbation to a map contained in this receiver. According to the period of the stabilized orbit in the receiver, the type of symbol that was transmitted over the communications channel can be determined. Therefore, the chosen type of the map's family is the key for deciphering the encoded information.

We now consider the basic principles of information processing based on the stable orbits of a perturbed map. Let a map orbit with period $\tau$ arise from a perturbation. The stability of this orbit is given by the relationship $\beta(p) = \prod_{i=1}^{\tau} D_x f(x_i, a_i)$, where $x_1 = f(x_\tau, a_\tau)$ and $x_{i+1} = f(x_i, a_i)$. If $|\beta(p)| < 1$, the orbit is stable. It is clear that, when $f(x, a)$ depends smoothly on the parameter, the space of perturbations $\mathbf{R}^\tau$ contains a certain region $U$ where a stable orbit is preserved.

Let us assume an information sequence that constitutes symbols of an alphabet, where every symbol is put in correspondence with a particular natural number. Let us find all possible perturbations leading to stable orbits with periods equal to such numbers. In other words, we localize in the perturbation space a subset $\mathbf{A}_\tau$ such that the perturbed map has a stable orbit with the prescribed period if $\hat{a} \in \mathbf{A}_\tau$. This encoding algorithm can be represented by the following scheme:

$$\left\{\begin{array}{c} Y \\ \text{symbol} \end{array}\right\} \longrightarrow \left\{\begin{array}{c} n_1,\ n_2,\ n_3 \\ \text{ASCII code} \end{array}\right\}$$

$$\longrightarrow \left\{\begin{array}{c} \{a_1, \ldots, a_{n_1+2}\},\ \{b_1, \ldots, b_{n_2+2}\},\ \{c_1, \ldots, c_{n_3+2}\} \\ \text{sets of parameters} \end{array}\right\} \longrightarrow \left\{\begin{array}{c} a_1, \ldots, c_{n_3+2} \\ \text{sequence of numbers} \end{array}\right\}$$

Thus, each of the symbols is associated with a set of periodic perturbations that give rise to a orbit with the desired period. As a result of transmission, perturbation in the form of a finite set of real numbers (parameters $a_1, a_2, \ldots, a_\tau$) arrives at the receiver. To decode (decrypt) the received symbol, this perturbation should be applied to the map used for encoding. The resulting perturbed map has a stable orbit, whose period can be determined by iteration from an arbitrary initial point. Thus, the encoded symbol is recovered. In this method, each information sequence consisting of a set of symbols is put in correspondence with the transmitted set of real numbers. Using the fact that every symbol may be encoded by a subset $\mathbf{A}_\tau$ rather than by a single perturbation $\hat{a}$, we may apply a different perturbation $\hat{a}' \in \mathbf{A}_\tau$ to each of the equal symbols in the transmitted sequence. Moreover, for most maps, subset $\mathbf{A}_\tau$ is a subspace of the perturbation space and, hence, perturbation $\hat{a}' \in \mathbf{A}_\tau$ may be selected at random. Therefore, although the original message may include identical symbols, the transmitted sequence looks absolutely random. This excludes the possibility of the transmitted information being decoded by an unauthorized user.

It is obvious that all the families of unimodal maps satisfy the conditions presented in Section 2. Since any orbit of the form $(x_c, x_2, x_3, \ldots, x_\tau)$ is stable for arbitrary $x_i \in \sigma$, the encoding and decoding algorithms can be implemented practically. The determination of $a_1, \ldots, a_\tau$ as solutions to system of equations (7) includes the following operations:

(i) Each symbol is put in correspondence with a particular map orbit $\tau$.

(ii) The values of $x_2, x_3, \ldots, x_\tau \in \sigma$ are arbitrarily chosen.

(iii) Equations (7) are used to calculate parameters $(a_1, a_2, \ldots, a_\tau) = \hat{a}$ for the set of points $(x_c, x_2, x_3, \ldots, x_\tau)$.

In this way, each of the symbols is associated with a parametric perturbation $\hat{a} = (a_1, a_2, \ldots, a_\tau)$. Owing to arbitrary selection of points $x_2, x_3, \ldots, x_\tau \in \sigma$, each of the repeated symbols may be encoded by sequence $x_2$, $x_3, \ldots, x_\tau$ that is randomly chosen from $\sigma$. Thus, the proposed method allows conversion of a symbol sequence into a numerical sequence, for example,

$$MAP\ldots \longleftrightarrow a_1, a_2, a_3, \ldots. \tag{9}$$

In view of the randomness of elements $x_2, x_3, \ldots, x_\tau$ and functional dependence (7), this numerical sequence is random. Now, numerical sequence (9) that is obtained is transmitted to a receiver. The decryption (decoding) of sequence (9) reduces to the extraction of sets $(a_1, a_2, \ldots, a_\tau)$ associated with particular symbols. This can be done readily since each of such sets corresponds to the stable orbit $(x_1, x_2, \ldots, x_\tau)$ with period $\tau$ and $x_1 = x_c$. Calculating the other elements $x_2 = f(x_c, a_1)$, $x_3 = f(x_2, a_2)$, $\ldots$, we arrive at a certain step to $x_{\tau+1} = f(x_\tau, a_\tau) = x_c$. The number of this step is the orbit period corresponding to the encoded symbol. The further decoding is nothing but a repetition of the above operation starting from step $a_{\tau+1}$: $\tilde{x}_2 = f(x_c, a_{\tau+1})$, $\tilde{x}_3 = f(\tilde{x}_2, a_{\tau+2})$, etc.

## 3. NUMERICAL INVESTIGATIONS OF THE ENCODING METHOD

To implement the encoding method described above, we consider the family of quadratic maps

$$x_{n+1} = ax_n(1-x_n). \tag{10}$$

This family is commonly used to model a wide range of physical systems (see, e.g., [40–43] and references therein). Furthermore, any unimodal map is semiconjugate to a quadratic map. Following (2), we introduce a $\tau$-periodic perturbation. In this case, it is convenient to represent perturbed map (10) in the form

$$\begin{cases} x_{n+1} = a_n x_n(1-x_n) \\ a_n = a_{n \bmod(\tau+1)}. \end{cases} \tag{11}$$

If this map has a orbit $p = (x_1, x_2, \ldots, x_t)$ with the period $t = \tau$, the orbit points obey the following system of equations: $x_2 = a_1x_1(1-x_1)$, $x_3 = a_2x_2(1-x_2)$, $\ldots$, $x_t = a_tx_t(1-x_t)$. To solve the inverse problem, i.e., to find the parameter values at which map (11) has orbit $p = (x_1, x_2, \ldots, x_t)$, it is necessary to solve the above equations for $a_i$:

$$\begin{gathered} a_1 = \frac{x_2}{x_1(1-x_1)}, \\ a_2 = \frac{x_3}{x_2(1-x_2)}, \ldots, a_t = \frac{x_1}{x_t(1-x_t)}. \end{gathered} \tag{12}$$

It is obvious that the condition $a_i \in [0, 4]$ does not hold true for all $x_i \in (0, 1)$. However, when it does hold true, there exist parameters $(a_1, a_2, \ldots, a_t)$ at which perturbed map (11) has orbit $p$ for each $p = (x_1, x_2, \ldots, x_t)$. When $|\beta(p)| = |\prod_{i=1}^{t} a_i(1-2x_i)| < 1$, this orbit is stable. In this case,

$$\begin{aligned} |\beta(p)| &= \left|\prod_{i=1}^{t} \frac{x_{i+1}}{x_i(1-x_i)}(1-2x_i)\right| \\ &= \left|\prod_{i=1}^{t} \frac{1-2x_i}{1-x_i}\right| < 1. \end{aligned} \tag{13}$$

Since we have $(1-2x_c)/(1-x_c) = 0$ for $x_c = 1/2$, inequality (13) can always be satisfied.

The sets of quantities $(x_1, x_2, \ldots, x_t)$ at which $a_i \in [0, 4]$ and inequality (13) holds true form a region in space, $\mathbf{R}^t$. Each point of this region corresponds to a stable orbit of the perturbed map. Using the expressions for $a_i$, $i = 1, 2, \ldots, t$, we have no difficulty in identifying this region in parametric space $\mathbf{R}^t$.

Let us consider the simplest case of a perturbation with period $\tau = 2$. It is obvious that the region of stable orbits in space $(x_1, x_2)$ is given by the following system of inequalities:

$$0 < \frac{x_2}{x_1(1-x_1)} \le 4, \quad 0 < \frac{x_1}{x_2(1-x_2)} \le 4,$$
$$\text{and} \quad \left|\frac{1-2x_1}{1-x_1}\frac{1-2x_2}{1-x_2}\right| < 1.$$

The first two inequalities are fulfilled for the set of all admissible orbits with a period of 2. The third inequality restricts this set to a subset where only stable orbits exist. To solve this inequality, we specify $x_1 \in (0, 1)$ and consider special features in the behavior of $x_2$. This yields the following conditions:

$$0 < x_2 < \frac{3x_1-2}{5x_1-3}, \quad 0 < x_1 < \frac{1}{3};$$

$$0 < x_2 < \frac{x_1}{3x_1-1}, \quad \frac{1}{3} < x_1 < \frac{3}{5};$$

$$\frac{3x_1-2}{5x_1-3} < x_2 < \frac{x_1}{3x_1-1}, \quad \frac{3}{5} < x_1 < 1.$$

Thus, we obtain the domain of existence for all stable orbits $p = (x_1, x_2)$ of map (11) with periods of 2 (Fig. 1a). The corresponding range of the values of parameters $(a_1, a_2)$ is obtained when the domain shown in Fig. 1a is transformed by formulas (12). A simple way to do this is to divide the domain in Fig. 1a into subdomains that admit the biunique mapping of these subdomains according to (12). Then, the domain boundaries are mapped under the condition that points inside the boundary get mapped to points inside. Note that transformation of this type leads to a singularity at point (0, 0). A detailed analysis shows that, for $\tau = 2$, mapping of the singularity into space $(a_1, a_2)$ results in the curve $a_2 = 1/a_1$.

The domain of existence of stable orbits $p = (x_1, x_2)$ with periods of 2 is shown in the parametric space $(a_1, a_2)$ in Fig. 1b. To reveal the details of map (12), the domain in Fig. 1a is divided by straight lines $x_1 = 1/2$ and $x_2 = 1/2$ into four portions denoted by different hatching. The corresponding subdomains in the space $(a_1, a_2)$ are hatched similarly. Since some domains in Fig. 1 overlap, map (12) is unique but not biunique. Moreover, the presence of overlapping regions suggests that, under certain perturbations, map (11) exhibits bistability and has two coexistent stable orbits.

In [39], range [3.8, 4.0] was thoroughly investigated for the possibility of chaos suppression. However, this range does not overlap the domains presented in Fig. 1b. For this reason, the orbits with periods of 2 were not discovered in map (11) at that time.

In the general case, i.e., under the action of perturbation with period $\tau > 2$, only the stable orbits in the form $p = (x_c, x_2, x_3, \ldots, x_t) = (1/2, x_2, x_3, \ldots, x_t)$ $(t = \tau)$ should be selected and used for calculating parameters $(a_1, a_2, \ldots, a_\tau)$. It is obvious that quadratic map (10) complies with all the requirements presented above. For this map, set $\sigma$ is the segment $[x_b, x_e]$, where $x_b$ and $x_e$ are the solutions to the equation $x_{\text{int}} = f(x, 4)$ and point $x_{\text{int}}$ is the intersection of curves $y = 4x(1 - x)$ and $y = x$; i.e., $[x_b, x_e] = [1/4, 3/4]$. Thus, when $a \in [0, 4]$ and $x \in [1/4, 3/4]$, the admissible errors in the parameters for the quadratic map can be estimated from

$$S_a = \max_{x,a}\left|\frac{\partial}{\partial a}f(x, a)\right| = \frac{1}{4},$$

$$S_x = \max_{x,a}\left|\frac{\partial}{\partial x}f(x, a)\right| = 2,$$

$$L = \max_{x,a}\left|\frac{\partial^2}{\partial x^2}f(x, a)\right| = 8.$$

The proposed encoding method can successfully be applied in a system for the encryption of symbols entered from a PC keyboard. Let us consider how to implement this for the MS-DOS operating system.[1] On IBM-compatible computers, each symbol entered from a keyboard is encoded by an integer. This number is an ASCII character and may take a value from 0 to 255. In particular, the ASCII characters from 65 to 90 and from 97 to 122 correspond to the capital and lowercase letters of the English alphabet, *A*–*Z* and *a*–*z*, respectively. The ASCII character set represents each symbol by three integers $n_1$, $n_2$, and $n_3$ satisfying the inequalities

$$0 \le n_1 \le 2, \quad 0 \le n_2 \le 9, \quad 0 \le n_3 \le 9.$$

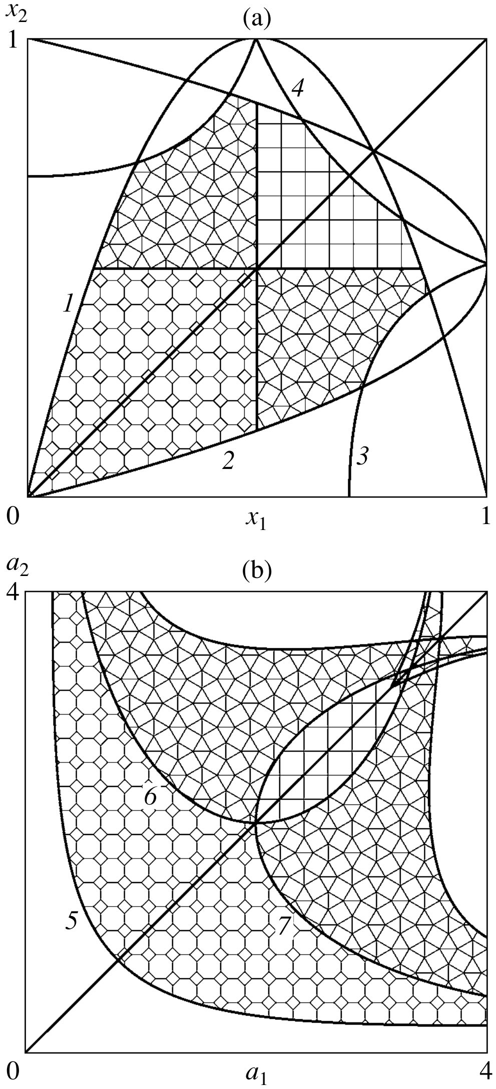

**Fig. 1.** The domain of existence for period-2 stable orbits of perturbed ($\tau = 2$) quadratic map (11) with the boundaries *(1)* $x_2 = 4x_1(1 - x_1)$, *(2)* $x_1 = 4x_2(1 - x_2)$, *(3)* $x_2 = (3x_1 - 2)/(5x_1 - 3)$, and *(4)* $x_2 = x_1/(3x_1 - 1)$ in plane $(x_1, x_2)$ and the boundaries *(5)* $a_2 = 1/a_1$, *(6)* $a_2 = 8/[a_1(4 - a_1)]$, and *(7)* $a_1 = 8/[a_2(4 - a_2)]$ in plane $(a_1, a_2)$.

[1] Note that the method can easily be adapted to the Windows operating system as well.

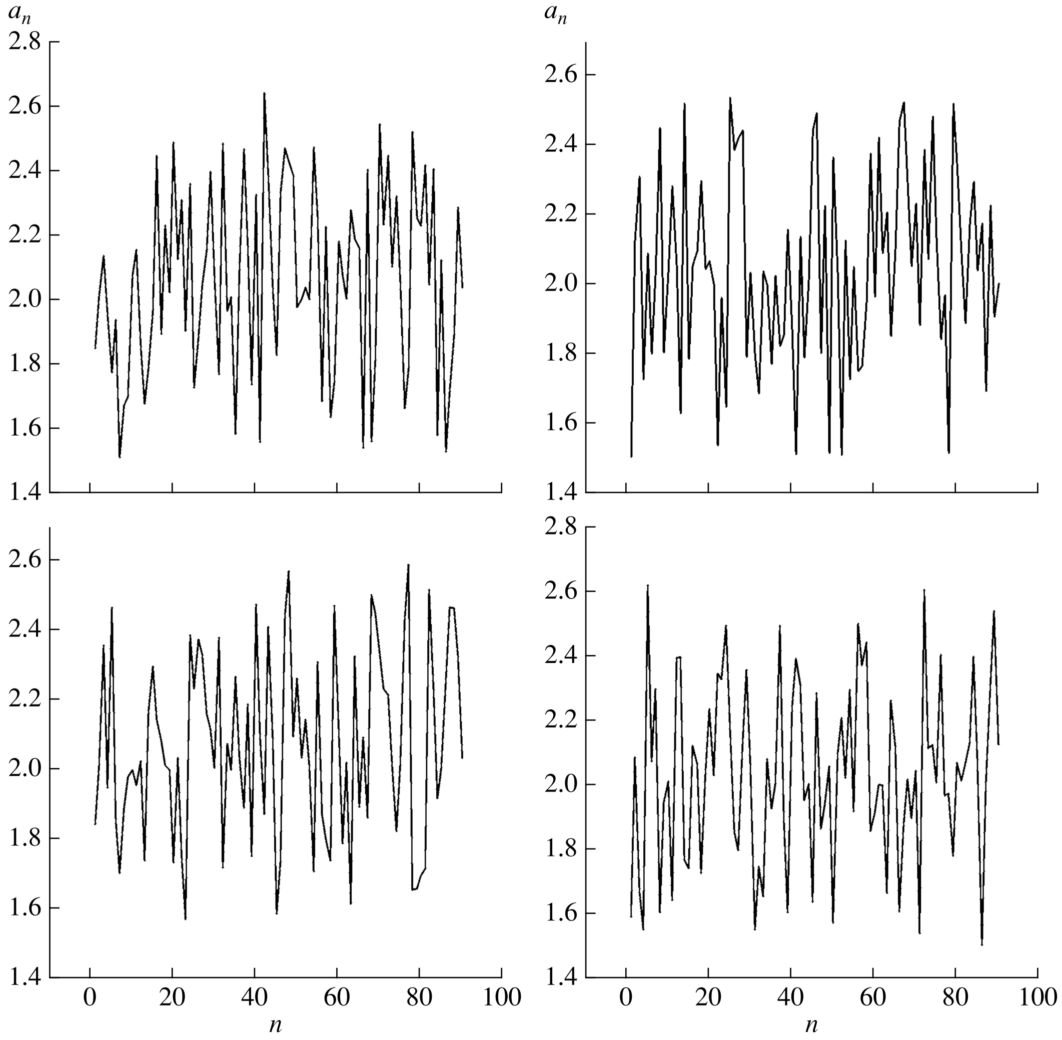

**Fig. 2.** Variants of numerical sequences encoding the word *CHAOS* with the use of a quadratic map.

For example, letter *A* with the ASCII character number 65 is represented by $n_1 = 0$, $n_2 = 6$, and $n_3 = 5$; letter *z* with the ASCII character number 122, by $n_1 = 1$, $n_2 = 2$, and $n_3 = 2$.

Now, we can formulate how the encryption system works:

(a) First, triad $n_1$, $n_2$, and $n_3$ is assigned to each symbol in accordance with its ASCII number.

(b) Each number in the triad is associated with a sequence of parameters stabilizing the orbit with period $n_i + 2$.

This algorithm is schematically represented by the flow chart below.

$$\begin{Bmatrix} Y \\ \text{symbol} \end{Bmatrix} \longleftrightarrow \begin{Bmatrix} t \\ \text{number} \end{Bmatrix}$$

$$\longleftrightarrow \begin{Bmatrix} T^t \\ \text{stable cycle} \end{Bmatrix} \longleftrightarrow \begin{Bmatrix} \text{set of} \\ \text{perturbations} \end{Bmatrix}$$

In the last step, there is a transition from the separate sets of parameters to a continuous sequence, which is transmitted to a receiver with a decipherer. The decipherer converts this sequence into a sequence of integers corresponding to the orbit periods. Diminishing each of the integers by two and grouping the sequence into sets of three, we easily reconstruct the ASCII character of a symbol and the symbol itself.

It is seen that any symbol can be encoded by using the stabilized orbits with periods from $\tau = t = 0 + 2 = 2$ to $\tau = t = 9 + 2 = 11$. Thus, the conditions for the applicability of the method are fulfilled (see Section 3) if the parameters are calculated with an error $\delta_a \le 10^{-8}$; hence, $\delta_x \le 10^{-4}$. In practice, owing to the inaccuracy of the parameter calculation, the exit condition $x_c = x_{k+1} = f(x_k, a_k)$ is substituted for inequality $|x_c - f(x_k, a_k)| \le \delta_x$. The intermediate points of a orbit $x_2, \dots, x_k$ are chosen to satisfy the condition $x_i \notin [x_c - \delta_x, x_c + \delta_x]$, $i = 2, \dots, k$.

The results of encryption are presented in Figs. 2 and 3. Figure 2 shows four different parameter

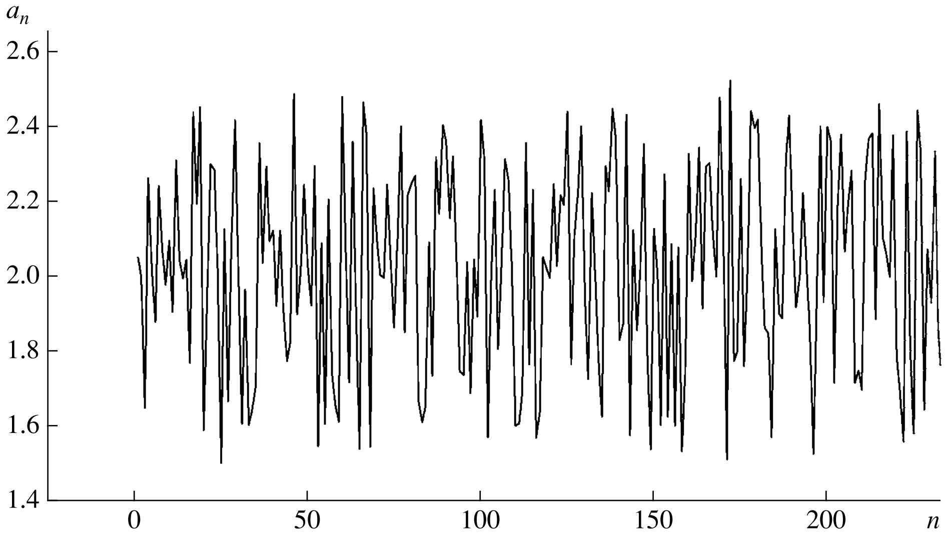

**Fig. 3.** Numerical sequence of encoding the ten letters *cccccccccc* with the use of a quadratic map.

sequences encoding the word *CHAOS*. Figure 3 depicts the parameter sequence encoding the text string of ten symbols *cccccccccc*.

The proposed method can be combined successfully with the keyboard entry of text messages and easily adapted to any other PC operating system.

## CONCLUSIONS

A new effective method is developed for hidden transmission of information encoded by preassigned stabilized orbits of 1D maps. The proposed method bears a partial resemblance to a well-known encryption method that uses a preassigned text source as the key in which each letter of the secret message is located and encoded by the numbers of the page, line, and column. However, the use of maps with strong chaotic properties makes the encryption process much more reliable. Furthermore, the capabilities of encryption based on a preassigned text source are always restricted by the size of the source, thereby allowing the decryption of information. On the contrary, the use of chaotic maps offers a theoretically infinite choice of the parameters.

In a particular implementation of the proposed method, when a family of unimodal maps is specified, it is possible to select perturbations that would stabilize the orbit passing through previously given points. In this case, the encoding, transmitting, and decoding of information can be automated easily, which is a significant advantage of the method. In this study, the algorithm is implemented on an IBM PC for the family of quadratic maps used as an example.

The main advantages of the method proposed for the hidden transmission of information include the following:

(i) A sufficiently wide class of maps, including multidimensional maps, may be used in practice.

(ii) No part of the information sequence itself appears in the communication channel; it is only the signal required for further processing that is transmitted.

(iii) The transmitted signal exhibits a purely random behavior, which provides for a high degree of data security.

(iv) No preliminary synchronization between a transmitter and a receiver is required.

(v) The method is stable against external interferences.

(vi) There is not only one signal sequence that may be assigned to the input information. Theoretically, the number of encoding variants is infinite.

Thus, (ii), (iii), and (iv) ensure a high degree of message security during transmission and (i), (v), and (vi) afford the widespread use of the method proposed. Moreover, since each symbol of a transmitted data sequence is associated with an entire region in the space of parameters, this method can be employed in the design of noise-immune information-processing systems.

The practical implementation of the hidden-transmission method also seems possible since the family of unimodal maps is readily modeled by means of standard electronic components. Thus, an operable integrated circuit (a chip) can be designed for practical purposes.

## REFERENCES

1. A. S. Dmitriev, Radiotekh. Elektron. (Moscow) **36**, 101 (1991).

2. A. Yu. Loskutov and V. M. Tereshko, *Artificial Neural Networks*, Ed. by I. Alexander and J. Taylor (Elsevier, Amsterdam, 1992), p. 449.

3. *Proceeding of the SPIE Annual Meeting on Chaos in Communications, San Diego, California, USA, 11–16 July 1993;* Proc. SPIE **2038** (1993).

4. A. Yu. Loskutov and V. M. Tereshko, *Neural Networks Applications*, Ed. by S. Gielen and B. Kappen (Springer, Berlin, 1995), p. 685.

5. S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993).

6. S. Hayes, C. Grebogi, E. Ott, and A. Mark, Phys. Rev. Lett. **73**, 1781 (1994).

7. H. D. I. Abarbanel and P. S. Linsay, IEEE Trans. Circuits Syst. **40**, 643 (1993).

8. D. Jianhua, Y. Huawei, and W. Lingan, Chin. Sci. Bull. **41**, 375 (1996).

9. A. S. Dmitriev, A. I. Panas, and S. O. Starkov, in *Proceedings of the International Conference on Nonlinear Dynamics, Nizhni Novgorod, Russia, 1996* (Izd. Nizhegorodsk. Gos. Univ., Nizhni Novgorod, 1996), p. 36.

10. Yu. V. Andreev, A. S. Dmitriev, and S. O. Starkov, IEEE Trans. Circuits Syst. **44**, 21 (1997).

11. A. S. Dmitriev, Yu. V. Andreev, and A. G. Bulushev, Zarubezh. Radioelektron., Usp. Sovrem. Radioelektron., No. 11, 27 (2000).

12. *Information Security Theory and Applications*, Ed. by P. D. Zegzhda (Yakhtsmen, Moscow, 1996) [in Russian].

13. *Introduction to Cryptography*, Ed. by V. V. Yashchenko (MTsNMO–CheRo, Moscow, 2000) [in Russian].

14. A. Yu. Loskutov, Yu. V. Mishchenko, and S. D. Rybalko, Voprosy Analiza Riska **2**, 2 (2000).

15. A. S. Dmitriev, L. V. Kuz'min, A. I. Panas, and S. O. Starkov, Radiotekh. Elektron. (Moscow) **43**, 1115 (1998) [J. Commun. Technol. Electron. **43**, 1038 (1998)].

16. G. Kolumbán, IEEE Trans. Circuits Syst. **47**, 1692 (2000).

17. G. Jakimovski and L. Kosarev, IEEE Trans. Circuits Syst. **48**, 163 (2001).

18. A. S. Dmitriev, B. E. Kyarginsky, A. I. Panas, and S. O. Starkov, Radiotekh. Elektron. (Moscow) **46**, 224 (2001) [J. Commun. Technol. Electron. **46**, 207 (2001)].

19. A. S. Dmitriev, B. E. Kyarginskii, A. I. Panas, and S. O. Starkov, in *Proceedings of the 9th Workshop on Nonlinear Dynamics of Electronic Systems, NDES'2001, Delft, Netherlands, 21—23 June 2001*, p. 157.

20. V. V. Alekseev and A. Yu. Loskutov, Dokl. Akad. Nauk SSSR **293**, 1346 (1987).

21. E. Ott, C. Grebogi, and J. A.Yorke, Phys. Rev. Lett. **64**, 1196 (1990).

22. A. Yu. Loskutov and A. I. Shishmarev, Usp. Matem. Nauk **48**, 169 (1993).

23. A. Yu. Loskutov and A. I. Shishmarev, Chaos **4**, 351 (1994).

24. R. Meucci, W. Gadovski, M. Ciofini, and F. T. Arecchi, Phys. Rev. E **49**, 2528 (1994).

25. A. Yu. Loskutov, S. D. Rybalko, and L. G. Akinshin, Differentsial'nye Uravneniya **34**, 1143 (1998).

26. A. Yu. Loskutov, Vestn. Mosk. Univ., Ser. 3: Fiz., Astron., No. 3, 3 (2001).

27. L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).

28. L. M. Pecora and T. L. Carroll, Phys. Rev. A **44**, 2374 (1991).

29. L. M. Pecora, T. L. Carroll, G. A. Johnson, and D. J. Mar, Chaos **7**, 520 (1997).

30. D. J. Sterling, Chaos **11**, 29 (2001).

31. V. S. Anishchenko and T. E. Vadivasova, Radiotekh. Elektron. (Moscow) **47**, 133 (2002) [J. Commun. Technol. Electron. **47**, 117 (2002)].

32. J. Gullicksen, M. de Sousa Vieira, M. A. Lieberman, *et al.*, in *Proceedings of the 1st Experimental Chaos Conference, 1–3 October 1991, Arlington, Virginia* (World Science, Singapore, 1992), p. 137.

33. *Proceedings of the International Conference on Acoustic, Speech, and Signal Processing* (IEEE, New York, 1992).

34. K. M. Coumo, A. V. Oppenheim, and S. H. Strogatz, Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 1629 (1993).

35. A. S. Dmitriev, G. Kassian, and A. Khilinsky, Int. J. Bifurcation Chaos Appl. Sci. Eng. **10**, 749 (2000).

36. A. Yu. Loskutov, *Nonlinear Dynamics: New Theoretical and Applied Results*, Ed. by J. Awrejcewicz (Akademie, Berlin, 1995), p. 126.

37. A. N. Derjugin, A. Yu. Loskutov, and V. M. Tereshko, Chaos, Solitons, and Fractals **7** (10), 1 (1996).

38. A. Yu. Loskutov, *Nonlinear Dynamics and Control,* Ed. by S. V. Emel'yanov and S. K. Korovin (Fizmatlit, Moscow, 2001), p. 163 [in Russian].

39. A. Yu. Loskutov, V. M. Tereshko, and K. A. Vasiliev, Int. J. Bifurcation Chaos Appl. Sci. Eng. **6**, 725 (1996).

40. Yu. I. Neimark and P. S. Landa, *Stochastic and Chaotic Oscillations* (Nauka, Moscow, 1987; Kluwer, Dordrecht, 1992).

41. J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields* (Springer, Berlin, 1990).

42. H. G. Schuster, *Deterministic Chaos* (Physik-Verlag, Weinheim, 1984; Mir, Moscow, 1988).

43. A. J. Lichtenberg and M. A. Lieberman, *Regular and Stochastic Motion* (Springer, New York, 1982; Mir, Moscow, 1984).