Nonlinear optical device for hidden information transfer: different versions

I.V. Izmailov and B.N. Poizner

Tomsk State University

Received October 7, 2001

A nonlinear ring interferometer (NRI) is chosen as a generalized structure model of encryption devices in nonlinear-dynamic cryptology. The suggested concept of chains of transposition points (CTP) allows NRI to be represented as a system, in which optical-physical interactions have the graph structure. For analysis and synthesis of similar systems, route-operator formalism is being proposed. Processes in the NRI are described and the model of a decoder exploiting a chaotic response is synthesized using this formalism. The possible foundations for classification of devices in nonlinear dynamic cryptography and different versions of such devices are given. Some examples of computer simulation of encryption/decryption in the static mode and the mode of dynamic chaos are presented and the effect of model parameters on the degree of communication confidentiality is illustrated. The concept of determined spatial chaos arising in the static mode of a dynamic system is discussed. A relation is found between the CTP and discrete maps.

Nonlinear ring interferometer and model of processes in it

In connection with the progress in laser physics and technology as well as in optical communication systems, it is necessary to develop methods and devices for hidden transmission of optical information.

A nonlinear ring interferometer (NRI) is an optical device involving phenomena related to both nonlinear dynamics (synergetics) and cryptology. Such devices were studied theoretically and experimentally by Akhmanov, Vorontsov, Larichev, Shmalgauzen, and other scientists (see Ref. 1). In the late 1980's – early 1990's, scientists of this research school proved the promise of the NRI as applied to information processing.

In the 1990's, the progress in synergetic methods gave rise to a new viewpoint on the problem of hidden information transfer, because the devices operating in the mode of deterministic (dynamic) chaos can distort the valid signal to such a degree that it can hardly be recognized. This opens up new possibilities of confidential communication with the use of chaotic modes in nonlinear systems. Since these systems may have different nature, it is reasonable to consider a new approach to scientific and technological field: nonlinear dynamic cryptology. The traditional cryptology historically is its first and most important part now. It is well known that cryptology consists of the following parts: cryptography dealing with mathematical methods of information conversion in order to protect it against illegal access and cryptanalysis, whose subject is various ways of illegal access, for example, cipher crack. Note that, in Doich's opinion, unpredictability caused by deterministic chaos is covered, in the general case, by quantum uncertainty (Ref. 2, p. 223). Thus, we formulate the problem of searching object domains, where cooperation of approaches of quantum and nonlinear dynamic cryptography is optimal.

Nonlinear dynamic cryptology demonstrates the expanding set of different versions of devices and operating modes, as well as methods for improvement of communication confidentiality.[3] Classification of the information transfer systems using chaotic signals was proposed by Vladimirov and Negrul in Ref. 4. According to literature data, cryptographic hidden communication systems are developed most rapidly in the radio wave frequency region.

In our opinion, the following problems are urgent in this context:

1) Justification of the possibilities of developing nonlinear dynamic cryptographic optical devices based on the knowledge of regularities of synergetic phenomena in optical systems. Examples of such justification by means of numerical simulation are given in Refs. 5–9.

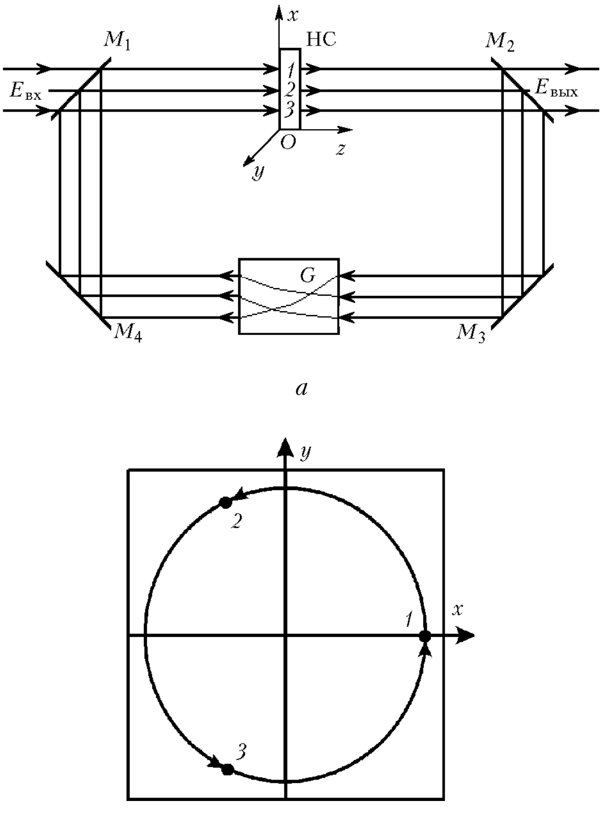
2) Use of the heuristic potential of methods for description of structural genesis in nonlinear optical systems[10–12] for the development of cryptology.

3) Mutual leasing (Ref. 13) of methods for description and organization of cryptography/cryptanalysis systems operating in the radio and optical regions.

4) Synthesis of optical logical elements based on bistable devices,[14] multibeam laser,[15] etc.

5) Practical implementation and optimization of nonlinear optical cryptology devices using laser radiation.

Within the framework of the first three problems (except for the cryptanalysis), let us consider a nonlinear ring interferometer. In our opinion, it may become an instrumental basis for nonlinear dynamic cryptology in optics.[5–7,9] To study this possibility, we used the model of structure formation in the laser beam cross section in NRI.[10] This model accounts for multiple passes of an optical field and amplitude and phase modulation of an input laser beam, as well as the time of field propagation in the NRI. The experimental geometry is depicted schematically in Fig. 1, where NE is a nonlinear element (Kerr medium), mirrors M_1 and M_2 have the power reflectance R, and the reflectance of mirrors M_3 and M_4 equals unity, G is a linear element serving for large-scale transformation of the field, for example, turn, shift, extension (compression) of a laser beam. Moreover, the element G can provide for splitting of the laser beam, turn, shift, extension (compression) of its parts, and then convergence into a single beam.



a

b

Fig. 1. Nonlinear ring interferometer. Element G turns the optical field by $\Delta = 120°$ (in the beam cross plane xOy), and the trajectories of three beams *1*, *2*, and *3* become closed after three passes over NRI (*a*); projection of closed trajectories of beams *1*, *2*, and *3* onto the plane xOy of beam cross section (*b*).

If the laser beam is not divided, the model has the form

$$\tau_n \partial U(\mathbf{r}, t)/\partial t = K\, A_{NE}^2(\mathbf{r}, \mathrm{t})/(1 - R) +$$
$$+ D_e \Delta_{xy} U(\mathbf{r}, t) - U(\mathbf{r}, t),$$
$$A_{NE}^2(\mathbf{r}, t) = (1 - R)\, A_{in}^2(\mathbf{r}, t) +$$
$$+ \gamma\, (1 - R)^{1/2} A_{in}(\mathbf{r}, t)\, \mathrm{A}_{NE}(\mathbf{r}', t - \tau) \times$$
$$\times \cos(\omega\tau + \varphi(\mathbf{r}, t) - \varphi_{NE}(\mathbf{r}', t - \tau))/\sigma +$$
$$+ [\gamma A_{NE}(\mathbf{r}', t - \tau)/(2\sigma)]^2, \qquad (1)$$

where $\mathbf{r} \equiv (x, y)$ is the radius vector of the cross section xOy; τ_n is the relaxation time of the nonlinear part of the refractive index of the Kerr medium (for example, liquid crystal) NE with the length L; D_e is the normalized diffusion coefficient of the molecules in the nonlinear medium; σ is the coefficient of beam extension by the element G; $\gamma = \gamma(\mathbf{r}', t)$ is the doubled loss coefficient; $K = (1 - R)\, n_2\, L\, |\mathbf{k}|\, A^2_{\max\,\{x,y,t\}}$ is the parameter determining the strength of nonlinear effects; n_2 is the parameter of nonlinear refraction; $|\mathbf{k}| = \omega/c$ is wavenumber; $A_{\max\,\{x,y,t\}}$ is the maximum value of the amplitude of the input field; A_{in} and A_{NE} are the field amplitudes normalized to $A_{\max\,\{x,y,t\}}$ at the entrance of NRI and NE, respectively; φ and φ_{NE} are the field phases at the entrance of NRI and NE, respectively; $\tau \equiv \tau(\mathbf{r}', t) = t_e(\mathbf{r}', t) + U(\mathbf{r}', t - t_e(\mathbf{r}', t))/\omega$, t_e is the equivalent delay time in NRI as measured by a modulator in the feedback unit (omitted in Fig. 1).

Description of ray route in nonlinear ring interferometer

If we ignore molecular diffusion in the NE (liquid crystal), then from Eq. (1) we can obtain a "point model" of the processes $U(\mathbf{r}, t)$ and $A_{NE}(\mathbf{r}, t)$ in the laser beam cross section xOy. The term "point model" is justified by the fact that the entire set of points in the cross section xOy, depending on the form of large-scale transformation of the field by the element G in the interferometer feedback unit, is divided into the infinite number of subsets. They are independent in the sense of the absence of physical interaction: between the fields $A_{NE}(\mathbf{r}, t)$; between the nonlinear phase changes $U(\mathbf{r}, t)$, as well as between $U(\mathbf{r}, t)$ and $A_{HC}(\mathbf{r}, t)$. But these subsets (belonging to the plane xOy) are *chains of points*, in which light fields and nonlinear phase changes interact consecutively (see Fig. 1).

In other words, the light signal (carried by an individual ray of a laser beam), while passing through the nonlinear medium and the NRI feedback unit at the point *i*, acquires the phase change U_i and experiences the delay t_{ei}. Because of the element G, the signal (ray) comes to the point $i + 1$. Here, in a sum with one of the input rays of the interferometer, it, according to model (1), affects the rate of variation of the nonlinear phase change U_{i+1}.

Just in this way the phase change U_i at the point i affects the phase change U_{i+1} at the point $i + 1$. We call such points *transpositional* points.[11] If the umber of points in the subsets mentioned above is finite and equal to m and the ray from the mth point comes to the first point, then we can speak about the degenerated two-dimensional relation of the mth order,[1] and the number m is called the transposition order. In such an organization of the feedback, the ray trajectory is closed after m passes in the NRI. According to the accepted method of numbering the transpositional points, the $i + 1$ record means the operation $((i + 1) \bmod m) + 1$, where $(i + 1) \bmod m$ denotes the residue of $i + 1$ division by m. Physically, this just means that the ray from the mth point comes to the first point.[11]

For example, according to Fig. 1*b*, the points *1*, *2*, and *3* form a *closed* chain of transpositional points (CTP), where $m = 3$. Speaking generally, at other transformation of the field by the element G in the NRI (see Fig. 1*a*), both closed and *unclosed* chains with different finite or infinite number of points is formed.

From the methodical viewpoint, the concept of CTP seems to be quite convenient, because the CTP structure represents the ray *path* through the NRI. The number of passes in the NRI serves a measure of the length of the passed route. It is natural to represent CTP as a graph. As known, graphs can be specified in different ways: by adjacency and incidence matrices, lists of, for example, pairs of nodes connected with ribs (arcs), specification of the set of adjacent nodes for every node [Ref. 16, p. 162]. The specific feature of optical and physical processes in the NRI is in the fact that the events of ray passages through NE and element G, where ray splitting is possible, as well as linear transformations and convergence of rays into a single beam form a strict sequence. To formalize this, we propose to use the following language for description of the chain structure.

(g_i) or (g) – point (graph node) g_i or g, which is a generator. That is, the term in parenthesis ( ) is a generator with respect to the next term.

$(g)\ i$ – ith point following the point g (ith descendant of the generator g). And $(g)\ 0 \equiv g$. But if it is followed by the symbol], then i is treated in other way.

$[(g)\ 0]_m$, $[(g)]_m$ – *branch* (branch point) of order m: at the point g one line branches into m lines.

$[(g)\ d]_m\ i$ – ith element (point) of dth subsequence starting at the branch point $[(g)]_m$. And $[(g)\ d]_m\ 0 \equiv [(g)]_m \equiv g$.

$[(g)\ d]_m\ \forall$ – dth subsequence (way, line) starting at the branch point $[(g)]_m$ (all elements (points) of the dth subsequence). And $[(g)\ d]_m\ 0 \in [(g)\ d]_m\ \forall$.

$[(g)\ d]_m$ – way segment (graph arc or rib) connecting the point g with the point $[(g)\ d]_m\ 1$. Hereinafter, for simplicity we make no difference between the terms of rib and arc.

$[(g)\ \forall]_m$ – any of way segments starting from the point g.

$\{(g)\}_m$ – *convergence* (point of convergence) of order m: at the point g, m lines converge into one.

$\{(g)\}_m\ i$ – ith element (point) of subsequence starting at the convergence $\{(g)\}_m$. And $\{(g)\}_m\ 0 \equiv \{(g)\}_m \equiv g$.

fin_i – final element of the chain, i.e., the point, at which the chain terminates, the subscript is the identifying number of the final point.

It is obvious that any point g is a branch point and, at the same time, the point of convergence of at least first order.

The absence of symbols between) and the following sign of convergence } makes unnecessary the presence of parenthesis ( ), i.e., the following identities are valid: $\{((g)\ i)\}_m \equiv \{(g)\ i\}_m$; $\{([(g)\ d]_n\ i)\}_m \equiv$ $\equiv \{[(g)\ d]_n\ i\}_m$, etc.

In some cases, open parenthesis can be omitted, but sometimes they should be kept. Let, for example, a branch of order 3 be at the point $(g_1)\ 4$. All generated sequences have different numbers of the elements n_1, n_2, and n_3, and they all overlap at one point, after which the chain terminates at the fifth element, i.e., the fifth element is the final one. Then this situation can be represented symbolically as $\{[(g_2)\ 1]_3\ n_1$; $[(g_2)\ 2]_3\ n_2$; $[(g_2)\ 3]_3\ n_3\}_3\ 5 = fin$, where $(g_1)\ 4 \equiv g_2$. If all subsequences have the same number of elements $(n_i = n)$, then this situation can be represented in a more compact form: $\{[(g_2)\ \forall]_3\ n\}_3 = fin$ or even $\{[(g_2)]_3\ n\}_3 = fin$.

Any expression having sense in the above context and using the proposed formalism specifies some route of a laser beam inside the NRI or a set of routes. A point is a route of zero length. This formalism allows us to judge on the number of branches and convergences (the number of routes) and the length of routes. In our opinion, a certain number of routes can serve as one of the ways to specify a graph.

Interferometer as a system with graph structure and route-operator formalism

Let us describe the simplest types of the chains of transpositional points that can exist in a nonlinear ring interferometer.

If the element G (see Fig. 1) reflects an image specularly about the straight line lying in the laser beam cross plane and passing through its center, then all CTP's are described as $(g_k)2 = g_k$, where k is the CTP identifier and $g_k \neq g_l$ at $k \neq l$ (hereinafter the subscripts k and l have the same meaning). For the points located at the line of specular reflection, $(g_k)1 = g_k$ is also true.

At laser beam shift by the distance Δx, the following expression is true: $(g_k)\ m_k = fin_k$, where $fin_k \neq g_k$ and m_k depends on Δx and on the position of the point g_k. For the square aperture of a laser beam and the shift $\Delta x = a/m$ along a square edge of the length a, all $m_k = m - 1$. It is obvious that CTP is unclosed, and its configuration can be called *linear*.

If the laser beam is turned by the angle $\Delta = 2\pi n/m$ in the plane xOy, $(g_k)\ m = g_k$ is true, in which n and m are coprime. It should be noted that for the beam center g_c we can assume $m = 1$ at any Δ. In this case, CTP is closed (in a ring) and its configuration can be logically called the *ring* one. It is obvious that if $m = 2$ ($\Delta = 180°$), then this expression reduces to that for the specular reflection.

If the turning angle $\Delta \neq 2\pi n/m$, then the CTP contains the infinite number of points, and the beginning and the end of the chain cannot be separated: $(g_{k,i})\ 1 = g_{k,i+1}$, where i is the number of a point in the chain, $i \in (-\infty; +\infty)$.

At compression of the laser beam ($\sigma<1$), the equations $\{(g_k)\ \infty\}_\infty = g_c$ and $\{(g_c)\ 1\}_\infty = g_c$ are true, therefore the CTP is a combined closed/unclosed configuration, which can be imagined as a "converging" infinite-pointed *star*.

At the extension of a laser beam ($\sigma > 1$), the equations $[(g_c)\ k]_\infty = \mathit{fin}_k$ and $(g_c)1 = g_c$ or $\{(\mathit{fin}_k)\ \infty\}_\infty = g_c$ and $(g_c)1 = g_c$ are true. The latter ones (contrary to the real chronology of ray passage over the NRI) describe the back route: from the final chain points fin_k located at the beam periphery to their common initial point g_c. The CTP is also combined, but its configuration can be imagined as a "diverging" infinite-pointed *star*.

Let us take into account that in the NRI there are points of input g_{in} and output $\mathit{fin}_{\text{out}}$ of the laser beam energy. For definiteness, we assume that the energy is released in the first way: $[(g_i)1]_m$.

Then for the case of specular reflection, omitting the subscript k, the equation $(g_k)\ 2 = g_k$ can be complemented as follows:

$$\{(g_{\text{in}\,i})\ 1;\ [(g_j)\ 2]_2\ 1\}_2 = g_i \quad \text{and} \quad [(g_j)\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,j}$$

or

$$[(\{(g_{\text{in}\,i})1;\ [(g_j)2]_2\ 1\}_2 = g_i\ )\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,i},$$

where $i, j = 1, 2$ or $2, 1$.

For the case of the beam shift, the equation $(g_k)\ m_k = \mathit{fin}_k$ is replaced with the three ones:

$$[((g_{\text{in}\,1})1 = g_1)\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,1},$$

$$[(\{\ (g_{\text{in}\,i})1;\ [(g_{i-1})\ 2]_2\ 1\}_2 = g_i)\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,i},$$

$$[(g_m)\ 2]_2\ 1 = \mathit{fin},$$

where $i \in [2; m]$. The third equation describes the fact that the CTP is unclosed, because the ray from the point g_m, entering the NRI feedback unit in the way denoted by the symbol 2: $[(g_m)\ 2]$, is absorbed at the point *fin* (for example, on the diaphragm).

For the case of beam turning by the angle $\Delta = 2\pi n/m$, the equation $(g_k)\ m = g_k$ is replaced by the following one:

$$[(\{(g_{\text{in}\,i+1})1;\ [(g_i)2]_2\ 1\}_2 = g_{i+1})\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,i+1},$$

where $i \in [1;\ m]$, and if $i + 1 = m + 1$, then the index should be equal to 1.

If $\Delta \neq 2\pi n/m$, then it is true that

$$[(\{(g_{\text{in}\,i+1})1;\ [(g_i)2]_2\ 1\}_2 = g_{i+1})\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,i+1},$$

where $i \in (-\infty; +\infty)$. In the case of the beam compression, in place of the equations $\{(g_k)\ \infty\}_\infty = g_c$ and $\{(g_c)1\}_\infty = g_c$, we have

$$[((g_{\text{in}\,1})1 = g_1)\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,1}$$

– for the initial CTP point g_1 lying on the periphery;

$$[(\{(g_{\text{in}\,i})1;\ [(g_{i-1})\ 2]_2\ 1\}_2 = g_i)\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,i}$$

– for internal CTP points g_i, where $i \in [2;\ m-1]$;

$$[(\{(g_{\text{in}\,m})1;\ [(g_{m-1})\ 2]_2\ 1\ \}_\infty = g_m\ )\ 1]_2\ 1 =$$

$$= \mathit{fin}_{\text{out}\,m},\ \{(g_m)1\}_\infty = g_m$$

– for the point g_m, being the limit g_c of the CTP sequence: at $m \to \infty$ $g_m \to g_c$.

In the case of beam extension in place of the pair of equations $[(g_c)\ k]_\infty = \mathit{fin}_k$ and $(g_c)1 = g_c$, we have

$$\{(g_{\text{in}\,c})1;\ [(g_c)\ 2]_\infty\ 1\}_2 = g_c,\ \ [(g_c)\ 1]_\infty\ 1 = \mathit{fin}_{\text{out}\,c}$$

– for the initial CTP point $g_1 = g_c$;

$$[(\{(g_{\text{in}\,2})1;\ [(g_1)\ 2]_\infty\ 1\}_2 = g_2)\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,2};$$

$$[(\{(g_{\text{in}\,i})1;\ [(g_{i-1})\ 2]_2\ 1\}_2 = g_i)\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,i}$$

– for the internal CTP points g_i, where $i \in [3;\ m)$;

$$[(g_m)\ 2]_2\ 1 = \mathit{fin}$$

– for the point g_m, being the limit of the CTP sequence at $m \to \infty$. And in place of the equations for the back route $\{(\mathit{fin}_k)\ \infty\}_\infty = g_c$ and $(g_c)1 = g_c$, the following equations are true:

$$[(\{(\mathit{fin}_{\text{out}\,m})1;\ (\mathit{fin})1\}_2 = g_m)\ 1]_2\ 1 = g_{\text{in}\,m}$$

– for the point g_m, being the limit of the CTP sequence at $m \to \infty$;

$$[(\{(\mathit{fin}_{\text{out}\,i})1;\ [(g_{i+1})\ 2]_2\ 1\}_2 = g_i)\ 1]_2\ 1 = g_{\text{in}\,i}$$

– for the internal CTP points g_i $i \in [2;\ m)$;

$$[(\{(\mathit{fin}_{\text{out}\,c})1;\ [(g_2)\ 2]_2\ 1\}_\infty = g_c\ )\ 1]_2\ 1 = g_{\text{in}\,c}$$

– for the initial CTP point $g_1 = g_c$.

In the above examples, the route equations fully specify the CTP structure in the NRI and the laser radiation entrance and exit points. It can easily be seen that for "ordinary" (internal) CTP points, the following route equation is valid:

$$[(\{(g_{\text{in}\,i+1})1;\ [(g_i)\ 2]_2\ 1\}_2 = g_{i+1})\ 1]_2\ 1 = \mathit{fin}_{\text{out}\,i+1}. \quad (2)$$

Apparently, the route equations should include description of physical transformations, the laser beam undergoes. For this purpose, route points and segments (graph nodes and ribs) should be assigned to some *operators* (transfer coefficients, functionals, etc.) describing physical processes in route elements. Thus, we can describe signal (a ray of a laser beam) transformations in graph elements.

As applied to the NRI (see Fig. 1), this is realized in the following way. Transpositional points g_i (convergence points) are located in the nonlinear medium. At these points, optical fields are summed, the resulting field is delayed, and the measure of this delay is the nonlinear phase change $U(\mathbf{r}, t)$ evolving under the effect of the resulting field according to the differential equation in the set (1).

Within the proposed *route-operator formalism*, this means that signals summed at the corresponding graph nodes acquire the phase delay $U_i(t)$. Because of the medium nonlinearity, the net signal changes the characteristics of the operator (transfer coefficient) realized at this node. It can easily be seen that the ribs $[(g_i)\ 1]_2$ and $[(g_{\text{in } i})\ 1]_1$ can be assigned to the transfer coefficient $(1-R)^{1/2}$, and the rib $[(g_i)\,2]_2$ can be assigned to the transfer coefficient at the amplitude $\gamma/2$ and the delay $t_{\text{e}\,i}(t)$. The final point of the ray *fin* located on the diaphragm will be described as an ideal absorber. For all the rest elements of the route, the default transfer coefficient equals unity, because no interaction with the laser beam field is assigned to these elements.

The operator corresponding to the input point $g_{\text{in } i}$ of the laser beam can be specified as a function of time and the index i representing the spatial dependence. This function must describe the signal (amplitude $A_i(t)$) dynamics at the NRI input.

It is natural to treat the beam output point $fin_{\text{out } i}$ as a place of the interface, i.e., NRI connection with other devices. Having known their characteristics, we can specify the operator corresponding to the point $fin_{\text{out } i}$. If such devices are absent, the point $fin_{\text{out } i}$ should be described as an ideal absorber.

Wide application of the route-operator formalism to synthesis of mathematical models is provided for by the general basic assumption that significant (in simulating) events of interaction in the system have the graph structure. Examples of such objects of the study can be easily found among optical, radio, and communication (both technical and sociocultural) systems.

Application of route-operator formalism to construction of a decoder model

If the NRI is interpreted as an encryption device, then the proposed formalism must serve a tool for synthesis of a dynamic system playing the role of a decoder. It is logical to consider the route equation relating the input and output NRI signals with the allowance for the operators realized by the route elements as *the equation for input signal* $A(\mathbf{r}, t)$. Let us describe our experience in that sort of synthesis.

First of all, it should be noted that now the point $fin_{\text{out } i+1}$ corresponds to the input of the decoder $fin_{\text{out}\, i+1} = g_{\text{in d}\, i+1}$ rather than an ideal absorber.

From the route equation (2) and the above assignment of operators to the elements of Eq. (2), it can easily be seen that the signal comes to the decoder output $fin_{\text{out } i+1}$ by the rib $[(g_{i+1})\ 1]_2$ with the transfer coefficient $(1-R)^{1/2}$. This means that the decoder must have an element, for example, the radiation input point $(g_{\text{in d } i+1})$, which realizes the operator $(1-R)^{-1/2}$ inverse to the operator of the decoder rib $[(g_{i+1})\ 1]_2$.

At the points g_i of the decoder, the signals coming from the ribs $[(g_{\text{in}\, i+1})\ 1]_1$ and $[(g_i)\ 2]_2$ sum up, undergo the delay $U_i(t)$, and separate. It should be noted that according to Eq. (2) and content of the operators, the results of separation are signals (at every output of the beam splitter) identical to the signal at its input. Consequently, the separation operation does not change the signal.

Then, two points must enter the decoder: phase delay $U_{\text{d } i+1}(t) = -U_{i+1}(t)$ occurs at the point $g_{\text{d } i+1}$. At the point $(g_{\text{d } i+1})1$, the signal equal to the signal S_i coming from the decoder rib $[(g_i)\ 2]_2$ is subtracted from the signal coming from the node $(g_{\text{d } i+1})$. Let the point $g_{\text{d } i+1}$ be located on the rib $[(g_{\text{in d } i+1})\ 1]_m$, i.e., $[(g_{\text{in d } i+1})\ 1]_m\ 1 = g_{\text{d } i+1}$, where the branch order m is determined below.

Let us take into account that the signal comes to the rib $[(g_i)\ 2]_2$ from the point (g_i) and it is equal to the signal coming from the point $(g_{\text{in d } i})$. Therefore, to generate the signal S_i in the decoder, it is sufficient to make the copy $[(g_{\text{in d } i})\ 2]_m$ of the rib $[(g_i)\ 2]_2$. This copy, however, has the difference that the phase delay realized on the rib $[(g_{\text{in d } i})\ 2]_m$ differs from $\omega t_{\text{e } i}(t)$ by π. In such a way, the operation of subtraction is provided for, now in the summator $(g_{\text{d } i+1})1$.

The decoder rib $[(g_{\text{in } i})\ 1]_1$ corresponds to the transfer coefficient $(1-R)^{1/2}$, therefore a terminal element compensating for radiation losses is needed in the decoder. Let the point $(g_{\text{d } i+1})1$ be such an element.

It is obvious that the necessary number of ways from the point $(g_{\text{in d } i})$ does not exceed two, i.e., it should be assumed that $m = 2$. With the allowance for the above-said, we can construct the equation describing the transformation of the signal in the decoder:

$$\{([(g_{\text{in d } i+1})\ 1]_2\ 1 = g_{\text{d } i+1})1;\ [(g_{\text{in d } i})\ 2]_2\ 1\}_2\ 1 = \\ = fin_{\text{out d } i+1}, \tag{3}$$

where the point $(g_{\text{in d } i+1})$ has the transfer coefficient $(1-R)^{-1/2}$; the point $(g_{\text{d } i+1})$ makes the phase delay $U_{\text{d } i+1}(t) = -U_{i+1}(t)$, the rib $[(g_{\text{in d } i})\ 2]_2$ has the transfer coefficient $\gamma/2$ and makes the phase delay $\omega t_{\text{e } i}(t) + \pi$. The convergence point $(g_{\text{d } i+1})1$ sums the incoming signals and transits them with the gain $(1-R)^{-1/2}$.

To provide for the delay $U_{\text{d } i+1}(t) = -U_{i+1}(t)$ in the decoder, it is sufficient to provide for fulfillment of the equality for the coefficients of decoder/encryption device nonlinearity $K_{\text{d}} = -K$ by selecting the nonlinear medium, for which $n_{2\text{d}} = -n_2$. But omitting selection of the nonlinear medium, for which $K_{\text{d}} = -K$, it is sufficient to provide for fulfillment of the conditions $\omega t_{\text{e d } i}(t) \approx \omega t_{\text{e } i}(t) + \pi$ and $\text{frac}\,(\omega t_{\text{e d } i}(t)/(2\pi)) = -\text{frac}(\omega t_{\text{e } i}(t)/(2\pi) + 0.5)$ in the rib $[(g_{\text{in d } i})\ 2]_2$, where frac denotes the fractional part of a number. In this case, the field at the decoder output has the same amplitude, and its phase is shifted by π with respect to the situation when $K_\text{d} = -K$.

Comparing Eqs. (3) and (2), we can notice their significant differences: the decoder at its input has a beam splitter rather than a summator as in the encryption device; and, vice versa, at its output the decoder has a summator rather than beam splitter. Having passed through the ribs $[(g_{\text{in d } i})\ \forall]_2$ of the decoder, all rays leave it, not coming back, i.e., the decoder turns out to be a nonlinear system *without feedback*, as in the encryption device. Therefore, only differential equation of the model (1) is true for the decoder, and the decoder itself cannot generate dynamic chaos. Thus, the decoder operates in the mode of *chaotic response*, or, using the terminology of Ref. 4, in the mode of passive synchronization. Let us restrict our further consideration to this case.

The decoder model (3) was synthesized based on the condition that the decoder completely reconstructs the signal $A_{\text{in } i}(t)$ at the NRI input from the signal at the NRI output: $A_{\text{in } i}(t) = A_{\text{out d } i}(t)$. If this requirement is reduced to the condition $A_{\text{out d } i}(t) = \text{const}\ A_{\text{in } i}(t)$, then the content of the operators realized by the route elements in the decoder model (3) can be changed.

For example, the point $(g_{\text{in d } i+1})$ has the transfer coefficient equal to unity; the point $(g_{\text{d } i+1})$ delays by $U_{i+1}(t)$. The convergence point $(g_{\text{d } i+1})1$ sums signals and transmits them with the transfer coefficient equal to unity. The decoder ribs $[(g_{\text{in d } i})\ 1]_2$ and $[(g_{\text{d}i})\ 1]_1$ have the transfer coefficient $(1-R)^{1/2}$. This, in its turn, requires the correcting $(1-R)$ times attenuation in the rib $[(g_{\text{in d } i})\ 2]_2$. This rib has the transfer coefficient $\gamma(1-R)/2$ and delays by $\omega t_{\text{e } i}(t) + \pi$. The encryption device rib $[(g_i)\ 1]_2$ and the decoder rib $[(g_{\text{in d } i})\ 1]_2$ have the transfer coefficient $(1 - R)^{1/2}$, therefore the decoder nonlinearity coefficient should be corrected according to the rule: $K_\text{d} = -K/(1 - R)^2$. For a decoder with such parameters, the following is valid: $A_{\text{out d } i}(t) = (1 - R)^2 A_{\text{in } i}(t)$. The decoder is depicted schematically in Fig. 2; the field amplitude in this case is corrected in the phase shifter π.

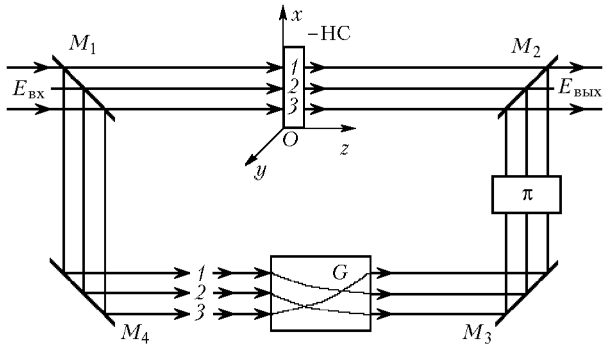


Fig. 2. Decoder layout. As the element G turns the light field by $\Delta = 120°$ (in the beam cross plane), the trajectories of the rays *1* and *3*, *2* and *1*, *3* and *2* after passage through the interferometer are summed on the exit mirror.

Different versions of nonlinear-dynamics cryptographic devices: classification

As is seen, the proposed formalism helps us to synthesize the decoder scheme based on the known route-operator scheme of the encryption device irrespective of its real design. Moreover, now the CTP structure, i.e., the structure of route equations, in particular, Eq. (2) and consequently Eq. (3), can serve a classifier for classification of already known versions and prediction of possible versions of cryptographic methods and devices of nonlinear-dynamic cryptology. It is known that such classifiers in cryptology are the following: key number (presence of an open key) and mathematical principles forming the basis for encryption/decryption.

It is obvious that such CTP characteristics of the encryption device as structure (closed, unclosed, combined), configuration (linear, converging/diverging star, ring, fractal, etc.), and number of points – communication channels (one, two, more than two, infinite number) can be extended to the corresponding classified pairs of encryption devices/decoders.

To be taken into account is also the operating mode of the encryption device (chaotic, static, etc.). For example, the static mode is inevitable at the unclosed CTP and at any constant signal at the encryption device input.

Other natural classifiers are the possibilities of simultaneous transmission of different messages: by one communication channel of a given chain (simultaneous phase and amplitude modulation), by different communication channels of a given CTP (through the way $g_{\text{in } i} \to fin_{\text{out d}i}$), by different sets of communication channels from different chains, as well fixation of one communication channel (one of the ways $fin_{\text{out } i} \to g_{\text{in d } i}$): for messaging, for synchronization, and for both these purposes simultaneously, as well as the channels intended for the above procedures.

The signal $S_i(t)$ coming to the point $g_{\text{in d}i}$ at the time t after various transformations in the decoder becomes the information signal $In_i(t) = F_{In\ i}(S_i(t - \tau_{In\ i}))$. But it can also serves the reference signal $B_i(t) = F_{B\ i}(S_i(t - \tau_{B\ i}))$. In addition, $S_i(t)$ plays the role of an external effect on different elements of the decoder, i.e., acts as a synchro signal. Depending on its function, the signal $S_i(t)$ can be called information masked, reference, or synchro signal.

The information signal $I_i(t)$ coming to the input $g_{\text{in } i}$ of an encryption device in the preceeding moments in time is separated as a result of the binary operation – subtraction:

$$I_i(t) = In_i(t) - B_j(t) =$$
$$= F_{In\ i}\,(S_i(t - \tau_{In\ i}) - F_{B\ j}\,[S_j\,(t - \tau_{B\ j})].$$

Note that the separation procedure may be based on different binary (+, ⊕, etc.) or, say, *N*th order operation.

In the separation of signal $I_i(t)$, the signal $S_i(t{-}\tau_{In\ i})$ is the information masked one, and the signal $S_j(t - \tau_{B\ j})$ is the reference one. At the same time, they both may be synchro signals, depending on whether they actually have the synchro effect on the decoder elements.

If the CTP is closed and consisting of a single point, then $i = j$. This corresponds to a single-channel (according to the classification from Ref. 4) system of confidential communication, although in the case of the NRI the number of CTP's is not limited. It should be noted that, in radio cryptographic systems using the chaotic response at decryption, the equality $In_i(t) = S_i(t)$ holds true and the nonlinear element is located in the feedback unit of the encryption device (see Ref. 17, Fig. 2*b*).

Thus, three functions of the signal S_i at separation of $I_i(t)$ are spaced in time: the signal S_i coming to the decoder in the period $(-\infty;\ t - \tau_{B\ i})$ first provides for its synchronization (first function). Then S_i plays the role of the reference signal $S_i(t - \tau_{B\ i})$ (second function). And then $S_i(t)$ carries an element of the message $I_i(t)$ (third function), which is separated due to the presence of the reference signal in the pre-synchronized decoder.

If the CTP is unclosed and consists of two points, i.e., $i \neq j$ (such a situation is possible in the NRI at a shift), $K = 0$ and a chaotic signal comes at the first point, whereas the information one comes at the second point, then this corresponds to the two-channel (with a separate channel for (passive) synchronization)[4] system of confidential communication. In the case of the NRI, the CTP number is still unlimited.

In the event of separation of the signal $I_2(t)$, the signal $S_2(t{-}\tau_{In\ 2})$ is an information masked one, and the signal $S_1(t - \tau_{B\ 1})$ is a synchro and reference one.

Thus, the three functions of the signal S_i at separation of $I_2(t)$ *are separated in time and space* (by channels 1 and 2): the signal S_1 coming to the decoder in the interval $(-\infty;\ t - \tau_{B\ 1})$ first provides its synchronization (first function). Then S_1 plays the role of the reference signal $S_1(t - \tau_{B\ 1})$ (second function). Then $S_2(t)$ carries the message $I_2(t)$ (third function), which is decrypted.

Separation of the functions of the S_i signal in time and/or space has an effect on the noise immunity of the communication system. Assume that additive noise affects a communication channel. Then, at separation of the S_i functions in space, the pernicious influence on the result of decryption is caused by the difference of the mean (over the propagation path) noise values $<N_i(t)>$ in the channels (for example, 1 and 2), where t is the time, at which the signal S_i comes at the *i*th decoder input. At separation in time, a significant factor is the change of the $<N_i(t)>$ level for the time $\Delta\tau = |\tau_{In\ i} - \tau_{B\ j}|$. Of course, here we should also take into account the effect of transformations $F_{In\ i}(S_i(t{-}\tau_{In\ i})$ and $F_{B\ j}(S_j(t - \tau_{B\ j}))$, the signals S_i and S_j undergo. But we restrict our consideration only to the allowance for the time $\tau_{In\ i}$ and $\tau_{B\ j}$.

It is obvious that the noise immunity in the single-channel communication system depends only on the change $<N_1(t + \Delta\tau)> - <N_1(t)>$. Generally speaking, $\Delta\tau$ is determined by the delay in the feedback unit of the encryption device.

In the two-channel communication system with a separate synchro channel, the noise immunity depends on $<N_2(t - \tau_{In\ 2})> - <N_1(t - \tau_{B\ 1})>$, i.e., on both these factors. However, time separation of the functions S_i can be eliminated by means of delay lines in both channels at the encryption device input and output. If the equality $\tau_{In\ 2} = \tau_{B\ 1}$ is achieved, only the space difference $<N_2(t)> - <N_1(t)>$ has an effect.

Thus, if the condition $<N_1(t + \Delta\tau)> - - <N_1(t)> \ll <N_2(t)> - <N_1(t)>$ or $<N_1(t + \Delta\tau)> - - <N_1(t)> \gg <N_2(t)> - <N_1(t)>$ is fulfilled, then a single- or two-channel system of confidential communication has an advantage in the relation to noise immunity. Note that Ref. 4 points to the advantage of the latter.

Apparently, different ratios between the numbers of channels (number of points in the CTP) intended for messaging and synchronization are possible in an NRI-based communication system. This gives rise to differences from the known systems. Let, for example, the laser beam be turned by the angle $\Delta = 2\pi n/m$ or undergo specular reflection in the NRI, i.e., a closed CTP takes place. If the nonlinear element in the encryption device and decoder is located just before the element G on the beam path (Fig. 3, where the field amplitude is corrected in the phase changer π), and $K_\text{d} = K/(1 - R)$, then the following situation is possible.

The communication channel $fin_{\text{out}\ i} \rightarrow g_{\text{in d}\ i}$ is used to transfer the signal S_i, which is both synchro and reference one with respect to the information masked signal S_{i+1} transmitted through the channel $fin_{\text{out}\ i+1} \rightarrow g_{\text{in d}\ i+1}$. In its turn, the signal S_{i+1} is used as a synchro and reference one with respect to the information masked signal S_{i+2} transmitted through the channel $fin_{\text{out}\ i+2} \rightarrow g_{\text{in d}\ i+2}$, etc. In other words, every signal S_i (channel $fin_{\text{out}\ i} \rightarrow g_{\text{in d}\ i}$) carries information and simultaneously serves a synchro and reference one for S_{i+1}. Thus, there is no need in service (only synchro) channels.

If the laser beam is shifted in the NRI, i.e., the unclosed CTP takes place, it is wise if the signal S_1 (channel $fin_{\text{out}\ 1} \rightarrow g_{\text{in d}\ 1}$) serves both the synchro and reference one, but caries no information. The rest signals and channels, as in the previous example, can play all the three parts. In this case, the fraction of the service channels is determined as the ratio $1/m$, where m is the number of CTP points. In the two-channel systems with a separate channel of (passive) synchronization,[4] this fraction equals 1/2.

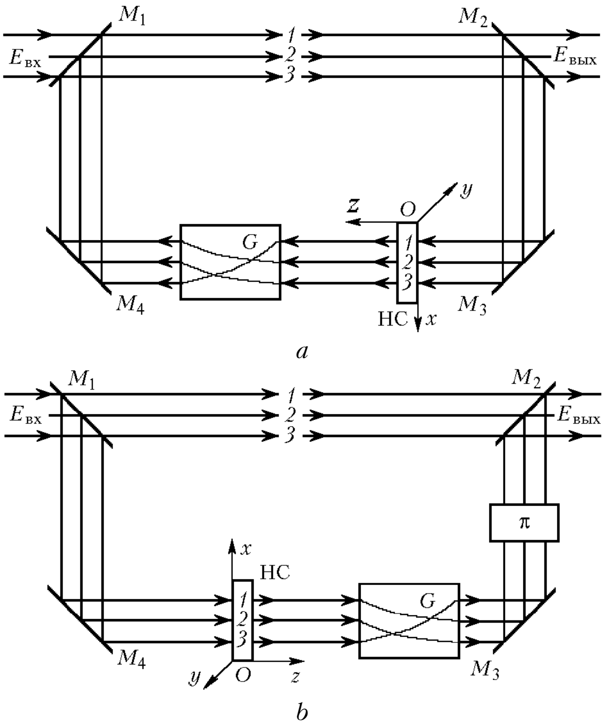


Fig. 3. Encryption device (*a*) and decoder (*b*) with NE in the feedback unit of encryption device. Ray trajectories correspond to the turn of the light field direction of propagation by the angle Δ = 120°.

Processes in the hidden optical information transfer system based on a pair of four-mirror interferometers – generators of deterministic spatiotemporal chaos were modeled in Ref. 8. In this system, the decoder operated in the mode of active synchronization. The model accounted for diffraction, a saturable absorber served as a nonlinear medium, and the depth of spatial amplitude modulation by the information signal was likely 0.005. The transfer of a static image was imitated. As a result of decryption, the image became rather distinguishable at the transfer coefficient of 0.7, but it was still reconstructed with some distortions.

Assume that the decoder output mirror *OM* in Fig. 4 in the system proposed in Ref. 8 is totally reflecting. Thus, the feedback in the decoder is broken, and it losses the capability of generating chaos and turns into the nonlinear discriminator. Assume also that the signals $M(x, t)$ and A_1 come to the encryption device not separately, but as a superposition (in the direction of $M(x, t)$ in Fig. 4). Correspondingly, the wave amplitude $A_2 = 0$. Then the structure of the pair of interferometers (encryption device + decoder) in Fig. 4 is almost equivalent to the pair of interferometers shown in Fig. 3, if the last element *G* is removed or it is assumed that Δ = 2π. If in Fig. 4 we increase the degree of nonlinearity of the decoder nonlinear element, then exact reconstruction of the signal probably becomes possible, similarly to that in the system shown in Fig. 3. Remind that in this paper we simulate the mode of chaotic response ignoring diffraction. It should be noted that an obvious disadvantage of the scheme shown in Fig. 4 is the requirement of coherence of the three laser beams: A_1, A_2, and $M(x, t)$.

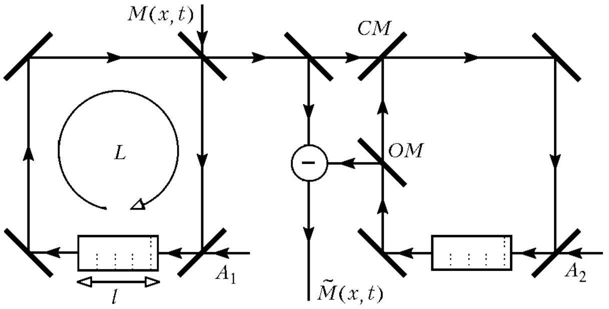


Fig. 4. Scheme of spatial and temporal information transfer using optical chaos.[8] *CM* and *OM* are communication and output mirrors; A_1 and A_2 are the amplitudes of the plane waves constantly coming to the resonators; $M(x, t)$ and tilded $M(x, t)$ denote the encrypted and decrypted signals; *l* is the length of the nonlinear element (saturable absorber); *L* is the optical length of the interferometers.

Imitation of hidden image transfer: mode of deterministic space-time chaos

Let us give some examples of imitation of image encryption/decryption by the method of computer experiment based on the models (1) and (3) as applied to confidential communication systems shown schematically in Figs. 1 and 2.

The results obtained for the case of closed CTP consisting of four points (Δ = 90°, $\tau_n = 10^{-9}$ s, $R = 0.5$, $t_e = \tau_n$, $\gamma = 0.5$) are shown in Fig. 5. Here the depth of spatial modulation of the laser beam amplitude equals 0.048, what is roughly ten times higher than in the model from Ref. 8. From this a possibility of decryption/encryption of a 2D image represented by a sequence of frames follows for the encryption device operating in the mode of deterministic space-time (dynamic, in other words) chaos. From visual analysis of the images shown in Fig. 5 we can conclude that:

– with the increase of time t/τ_n, the signal hiding increases;

– the period of encryption device "warming-up" is no less than $5\tau_n$;

– hiding and the rate of its increase depend on the NRI parameters.

The increase in the signal hiding with the increase of the nonlinearity coefficient *K* of the NRI can be estimated by the methods of spectral analysis considering Figs. 6 and 7. These figures show time realizations, phase portraits, and Fourier spectra of the wave amplitude A_i at the output, where *i* is the number of the transpositional point in the CTP, $D_e = 0$.

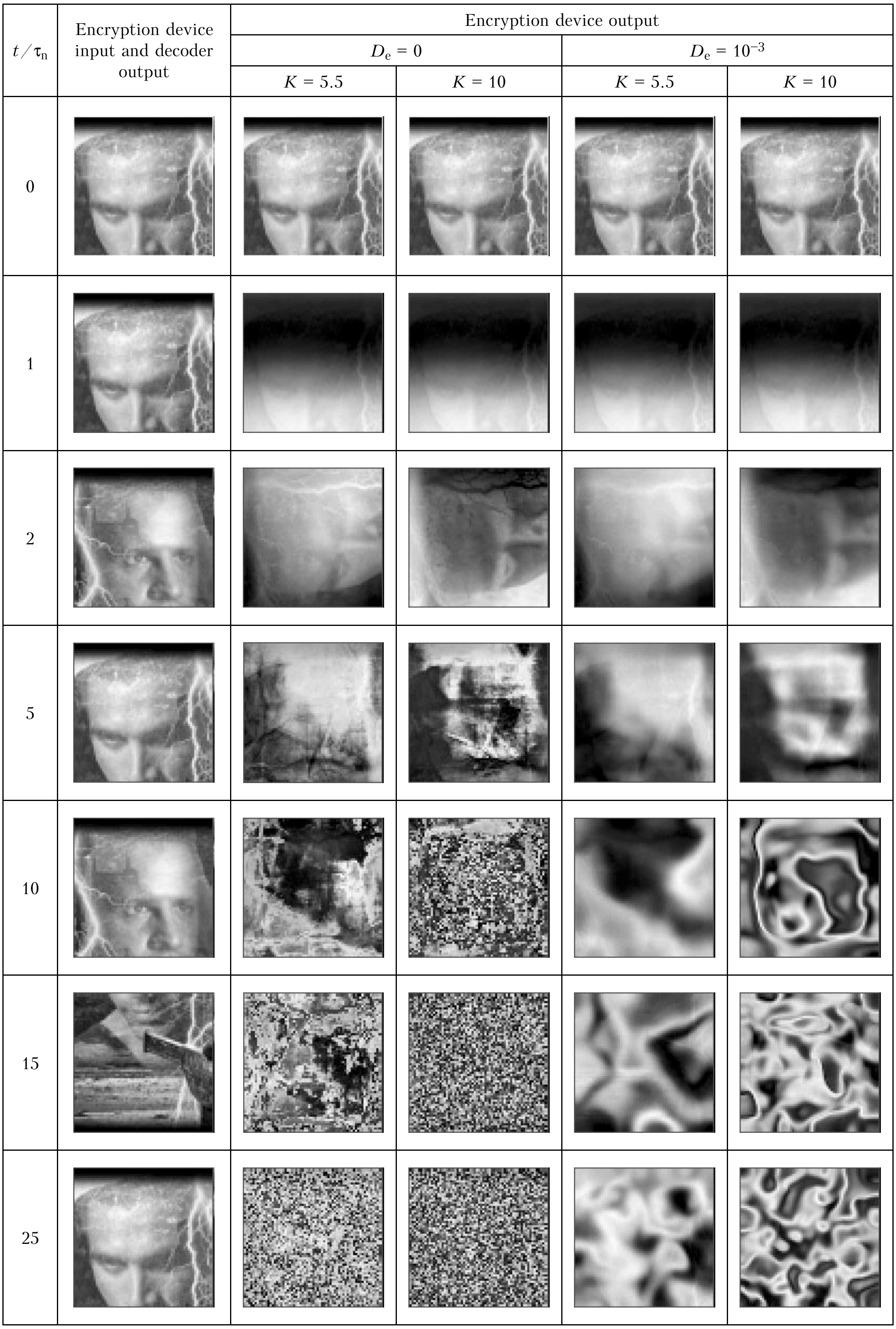


Fig. 5. Frames of the process of imitation of image encryption/decryption in the mode of dynamic chaos at different values of the nonlinearity coefficient K and the normalized diffusion coefficient D_e in NRI.

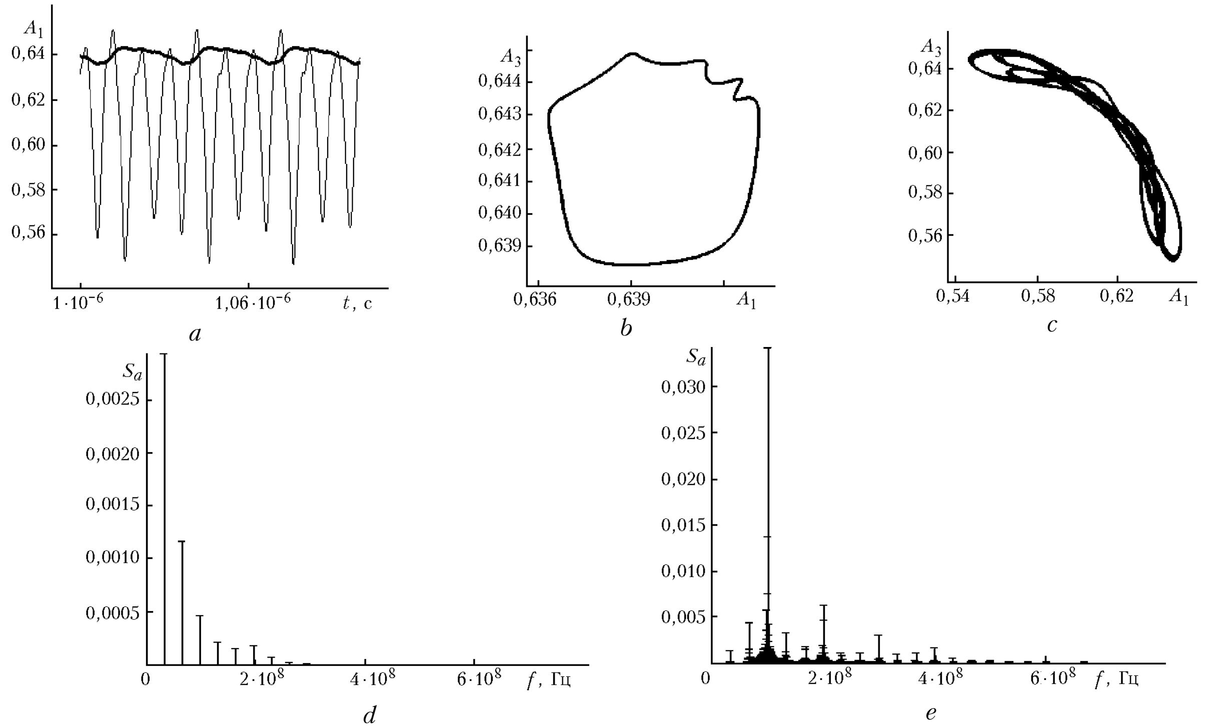


Fig. 6. Time realization of A_1 (*a*), phase portraits (*b*, *c*), Fourier spectra S_a of the output wave amplitude A_1 (*d*, *e*) in the free running mode (*a* (bold curve), *b*, *d*) and the mode of amplitude modulation (*a* (thin curve), *c*, *e*). $A_1 = A(\mathbf{r}, t)$, where $\mathbf{r} = (0.5, 0)$; $A_3 = A(\mathbf{r}, t)$, where $\mathbf{r} = (0, 0.5)$. $K = 4.55$. The modulation law: $A_{\text{in}}(\mathbf{r}, t) = [1 + 0.01 \cdot \cos(2\pi f_1\, t)]/1.01$, where $f_1 = 1/(30.618 \cdot 10^{-9}) \approx 0.3266 \cdot 10^8$ corresponds to the frequency of the Fourier spectrum harmonic having the maximum amplitude (*d*).

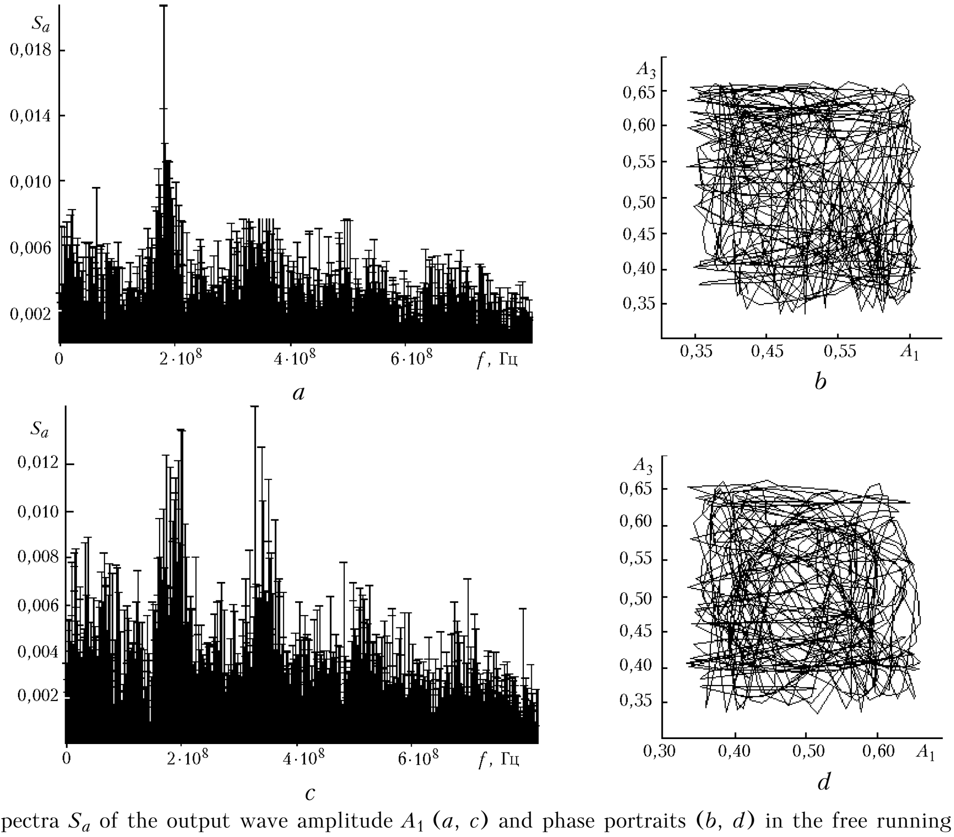


Fig. 7. Fourier spectra S_a of the output wave amplitude A_1 (*a*, *c*) and phase portraits (*b*, *d*) in the free running mode (*a*, *b*) and the mode of amplitude modulation (*c*, *d*) at the same parameters as in Fig. 6. $K = 10$.

Imitation of hidden image transfer: mode of deterministic spatial chaos

Figure 8 proves the possibility of encryption /decryption of a 2D image with the encryption device operating in the *static mode*. The signal hiding in this case depends on the NRI parameters. The static mode meaning the absence of changes in time does not exclude, however paradoxical it is, randomization of a static spatial structure (two-dimensional, three-dimensional, N-dimensional). Therefore, we propose to call this phenomenon *deterministic spatial chaos*. The term "deterministic," as generally accepted, points to the fact that disorder obeys some regularity dictated by the mathematical model, rather than originates from a random factor. In this way, we emphasize the analogy/contrast with the widely known temporal, i.e., dynamic (deterministic), chaos in the models of one-dimensional systems and the space-time chaos, or turbulence, in the models of multidimensional systems. The deterministic spatial chaos naturally opposes the spatial order demonstrated by objects possessing some symmetry, fractals, etc. Visual analysis of Fig. 8 evidences the principal possibility of existence of the deterministic spatial chaos.

Chain of transpositional points as an equivalent of discrete mapping

In our case, the deterministic spatial chaos is realized in the model consisting of algebraic equations (or equalities for unclosed CTP) following from Eq. (1), when $\partial U(\mathbf{r}, t)/\partial t = 0$ and $D_e \Delta_{xy} U(\mathbf{r}, t) = 0$. As was shown above, the route-operator equation (2) is an equivalent of the algebraic equations (or equalities). In this case, it is proposed to consider the values of the dynamic variable ($U(\mathbf{r}, t)$ or laser beam amplitude $A_{NE}(\mathbf{r}, t)$) at CTP points as its values at the points of the discrete map. Thus, we establish a relation between the differential equations for the static mode and discrete maps. In our opinion, it is an *alternative* of the classic relation[18,19] between the differential equations for the dynamic mode and the maps based on Poincare cross sections. Therefore, it is logical to treat the number of a transpositional point in the chain as a discrete evolutional variable.

In the dynamic mode, the values of the dynamic variable ($U(\mathbf{r}, t)$ or $A_{NE}(\mathbf{r}, t)$) at CTP points also can be treated as its values at the points of the discrete map. But in this case, besides the traditional discrete evolutional variable (the number of a transpositional point in the chain), a map has a continuous evolutional variable (time t in the model (1) or (2)) responsible for transformation of the CTP as a whole. It is obvious that the relation between the values of the dynamic variable at the points of such a discrete map becomes not so trivial, as in the static mode. As applied to the NRI, this relation is present implicitly in the model (1) and explicitly in the model (2). Thus, the problem of studying processes in the NRI within one CTP can be reformulated as a problem of *studying the evolution of discrete maps*.

If the CTP is closed, then discrete mapping turns out to be periodic with the period equal to the number of the CTP points. The unclosed CTP assumes four possibilities: (1) finite number m of CTP points; (2) infinite number ($m = \infty$) of CTP points in the chain having such a point numeration that: (a) the number of the initial point is 1 and the number of the end point is ∞, (b) the number of the end point is 1, and the number of the initial point is $-\infty$, (c) the numbers of the initial and the end points are respectively $-\infty$ and ∞. As far as we can judge, in the cases (b) and (c), when the first point is unknown, one has to deal with a rather specific problem, for example, within the framework of the model (1) and (2): if we would like to know the evolution of at least one point in a chain, then we have to take into account the effect of the *infinite* number of points preceding it in the CTP.

It is clear from physical reasoning that operation of the encryption device can be characterized by the "warming-up" period τ_h (in the mode of space-time chaos) and the period of establishment τ_r (in the static mode), whereas the decoder operation can be characterized by the period of synchronization establishment τ_s. Let us consider the estimation of the efficiency of these devices in the above modes for the cases of transfer of a single image or a series of images.

If only one image is to be transferred, then the time needed for encryption in the static mode is determined by the time τ_r of establishment of the processes in the encryption device (NRI). This time depends, in particular, on the CTP length. In this case, the receiving part has to receive only the established image at the encryption device output (cryptogram) for decryption. Therefore, if the decoder is equipped with a device for cryptogram storage, then the message length τ_m is determined by its speed. If there is no such a device, then $\tau_m = \tau_s$. The time needed for decryption is determined by the time needed for establishing synchronization τ_s.

Two versions are possible in the mode of space-time chaos. If the encryption device and decoder are pre-synchronized, i.e., the corresponding initial conditions are preset in them, then the time needed for encryption, for decryption, and τ_m are determined by the "warming-up" period τ_h. Otherwise, the decryption time and τ_m are determined by the time τ_s, and the encryption time is equal to the largest of τ_h and τ_s.

If a series of images is to be transferred, then the process of transfer of every image in the static mode is identical to transfer of a single image. In the mode of space-time chaos, the transfer of the first image is also identical to the transfer of a single image. The following images can be transferred as fast as allowed by image change rate and recording units (possible decrease or increase in cryptographic resistance at that fast transfer is not considered here).

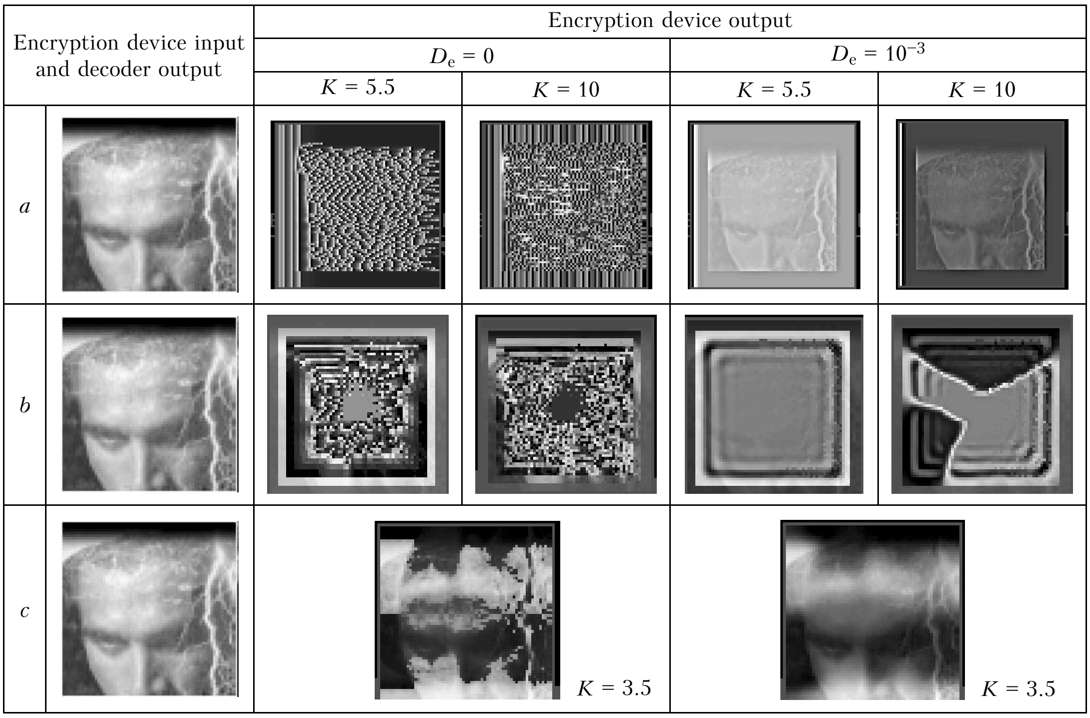


Fig. 8. Imitation of image encryption/decryption in the static mode of NRI at different values of the nonlinearity coefficient K and the normalized diffusion coefficient D_e. The laser beam in the NRI feedback unit is subject to shift along the axis Ox by 1/80 (*a*), compression $\sigma = 0.9$ (*b*), specular reflection about the axis Ox (*c*).

It is reasonable to believe that the following inequality is fulfilled: $\tau_s < \tau_h < \tau_r$. Then the static mode seems *preferable*, if the limiting factor is the capacity or price of the communication channel, as well as if the task is to store information in the encrypted form.

Obviously, simulation of an optical device of nonlinear dynamic cryptography leads to the problem of multiparameter optimization of this device and its possible analogs and versions.

Conclusion

In this paper, we have justified the possibility of and outlined the ways for developing optical devices of nonlinear dynamic cryptography using, as an example, a nonlinear ring interferometer.

Some methods of description and organization of radio and optical systems of nonlinear dynamic cryptography have been leased. In particular, the nonlinear ring interferometer (see Fig. 1) has been interpreted as a generalized structure model of encryption devices. The route-operator description forms the basis for such generalization. Further development of this approach has allowed us to propose new bases for classification and versions of implementation of hidden information transfer based on devices of nonlinear dynamic cryptography.

The operation with the concept of CTP (chain of transpositional points) has served as a basis for the use of the theory of graphs. As a result, we have succeeded in constructing the language for CTP description. On its basis, we have developed the route-operator formalism oriented at the study of systems, whose physical interactions have the structure of a graph, in particular, ring systems. The model of process in the NRI-based encryption device has been described within this formalism [route-operator equation (2)]. If such models are treated as equations for the unknown input signal, this can serve the methodology for synthesis of the route-operator model of the decoder using a chaotic response. Application of this methodology has led us to the decoder model (3) and, in its turn, to the optical scheme of the device of nonlinear-dynamic cryptography (see Fig. 2).

A version of the decoder model (see Fig. 3) has been compared with the scheme of space-time relation in the mode of chaos synchronization[8] (see Fig. 4), and disadvantages of the latter and the ways of its transformation into the scheme shown in Fig. 3 have been demonstrated.

The efficiency of operation of the encryption device has been estimated in the mode of space-time chaos and in the static mode.

The relation of the CTP with the discrete maps has been revealed for the static and dynamic modes. The possibility of formulation of the problem on evolution of discrete maps as an instrument for studying processes in the NRI within one CTP has been demonstrated.

The concept of deterministic spatial chaos arising in the mode of a dynamic system, for example NRI, has been put forward.

Some examples of computer imitation of encryption/decryption of two-dimensional images in the modes of space-time and spatial chaos have been presented (see Figs. 5 and 8). The influence of nonlinearity on the degree of communication confidentiality in the mode of space-time chaos has been analyzed with the use of Fourier spectra and phase portraits (see Figs. 6 and 7).

On the whole, the heuristic potential of the route-operator formalism has been demonstrated as applied to the study of signal transfer in optical nonlinear ring systems.

Acknowledgments

The authors are thankful to S.N. Vladimirov and V.V. Negrul who called our attention to Ref. 3 and A.A. Rybak who pointed out Ref. 8.

This work was partly supported by the Russian Foundation for Basic Research (Project No. 01–02–06175) and the Ministry of Education of the RF (Project No. 99 06 75 within the framework of the Program "Basic Researches of Higher School in Natural Sciences and the Humanities. Universities of Russia").

References

1. S.A. Akhmanov and M.A. Vorontsov, eds., *New Physical Principles of Optical Processing of Information* (Nauka, Moscow, 1990), pp. 263–326.
2. D. Doich, *Structure of Reality* (Izhevsk, 2001), 400 pp.
3. M. Khasler, Usp. Sovr. Radioelektron., No 11, 33–43 (1998).
4. S.N. Vladimirov and V.V. Negrul, in: *Proceedings of the Fifth International Conference on Urgent Problems of Electronic* (Novosibirsk, 2000), Vol. 7, pp. 39–41.
5. I.V. Izmailov, B.N. Poizner, and M.A. Shulepov, in: *Abstracts of Reports at the Fourth International Conference on Mathematical Models of Nonlinear Excitations, Transfer, Dynamics, and Control in Condensed Systems and Other Media,* Moscow (2000), p. 50.
6. I.V. Izmailov, B.N. Poizner, and M.A. Shulepov, "*Modulation and demodulation of optical signals using nonlinear ring interferometer,*" Dep. VINITI, No. 1865–V00, July 4, 2000.
7. I.V. Izmailov, B.N. Poizner, and M.A. Shulepov, in: *Proceedings of International Optical Congress on Optics XXI,* St. Petersburg (2000); *Conference on Fundamental Problems of Optics,* St. Petersburg (2000), pp. 30–31.
8. J. Garcia-Ojalvo and R. Roy, *Spatiotemporal Communication with Synchronized Optical Chaos,* http://xxx.lanl.gov/abs/nlin.CD/0011012.
9. I.V. Izmailov and M.A. Shulepov, Proc. SPIE **4513**, 46–51 (2001).
10. I.V. Izmailov, "*Model of processes in nonlinear ring interferometer that accounts for delay, loss, energy density transformation, and multiple passes of non-monochromatic field,*" Dep. VINITI, No. 3865–B97, December 31, Moscow (1997).
11. I.V. Izmailov, A.L. Magazinnikov, and B.N. Poizner, Atmos. Oceanic Opt. **13**, No. 9. 747–753 (2000).
12. S.S. Chesnokov and A.A. Rybak, Laser Phys. **10**, No. 5, 1–8 (2000).
13. E.A. Sosnin and B.N. Poizner, in: *Proceedings of the First All-Russia Conference on Integration of Education and Basic Research in Universities: Innovation Strategies and Technologies*, (Tomsk State University Publishing House, Tomsk, 2000), Vol. 1, pp. 115–118.
14. N.N. Rozanov, *Optical Bistability and Hysteresis in Distributed Nonlinear Systems* (Nauka, Moscow, 1997), 336 pp.
15. G.S. Evtushenko, B.N. Poizner, E.A. Sosnin, and V.F. Tarasenko, *How to Begin Working in Scientific Community.* Student's Book (Tomsk University Publishing House, Tomsk, 1998), 140 pp.
16. Yu.V. Prokhorov, ed., *Mathematical Encyclopedic Glossary* (Sov. Entsiklopediya, Moscow, 1988), 847 pp.
17. S.N. Vladimirov and V.V. Negrul, Izv. Vyssh. Uchebn. Zaved., Ser. Prikl. Nelinein. Dinam. **8**, No. 6, 53–64 (2000).
18. V.S. Anishchenko, T.E. Vadivasova, and V.V. Astakhov, *Nonlinear Dynamics of Chaotic and Stochastic Systems. Fundamentals and Selected Problems* (Saratov University Publishing House, Saratov, 1999), 368 pp.
19. A.P. Kuznetsov, Soros. Obraz. Zh., No. 11, 104–110 (2000).