Secure steganographic communication algorithm based on self-organizing patterns

Loreta Saunoriene[*] and Minvydas Ragulskis[†]
Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-222, Kaunas LT-51368, Lithuania
(Received 9 June 2011; revised manuscript received 22 August 2011; published 18 November 2011)

A secure steganographic communication algorithm based on patterns evolving in a Beddington-de Angelis-type predator-prey model with self- and cross-diffusion is proposed in this paper. Small perturbations of initial states of the system around the state of equilibrium result in the evolution of self-organizing patterns. Small differences between initial perturbations result in slight differences also in the evolving patterns. It is shown that the generation of interpretable target patterns cannot be considered as a secure mean of communication because contours of the secret image can be retrieved from the cover image using statistical techniques if only it represents small perturbations of the initial states of the system. An alternative approach when the cover image represents the self-organizing pattern that has evolved from initial states perturbed using the dot-skeleton representation of the secret image can be considered as a safe visual communication technique protecting both the secret image and communicating parties.

DOI: 10.1103/PhysRevE.84.056213 PACS number(s): 82.40.Ck, 95.75.Mn

I. INTRODUCTION

The evolution of complex patterns in simple systems has attracted the attention of researchers for a long time. One of the classical numerical examples illustrating a surprising variety of irregular spatiotemporal patterns comprises a simple reaction-diffusion model with finite amplitude perturbations [1]. The phenomenology of a wide variety of two- and three-dimensional physical-chemical systems displaying prevalent stripe and bubble morphologies of domain patterns in equilibrium is discussed in Ref. [2]. It is shown that small perturbations of initial states of the system play a central role in the initiation of pattern formation process [3].

The physics of pattern formation remains an active research area. It is shown that the reaction-diffusion model serves as a framework for understanding biological pattern formation in [4]. Pattern formation mechanisms of a reaction-diffusion-advection system, with one diffusivity, differential advection, and Robin boundary conditions of the Danckwerts type, are investigated in Ref. [5]. It is shown that time-delay-induced instabilities in reaction-diffusion systems result in stationary patterns and Turing-Hopf transition with the formation of spirals [6]. Time-periodic forcing of spatially extended patterns near a Turing-Hopf bifurcation point is studied in Ref. [7]. A method to characterize and distinguish patterns from inclined water-oil flow experiments based on the concept of network motifs is proposed in Ref. [8]. An analytic study of traveling fronts, localized colonies, extended patterns, the well-known Allee effect, and spatially nonlocal competition interactions arising from a reaction-diffusion equation is presented in Ref. [9]. The pattern transition from target waves to spiral waves upon the increment of inactive beads in a discrete system model, where ion-exchange resin loaded with a Belousov-Zhabotinsky catalyst corresponds to the active beads, is studied in Ref. [10]. Patterns specifying dynamic behavior of chemoresponsive gels undergoing the Belousov-Zhabotinsky reaction are constructed in Ref. [11]. Investigation of disordered plane waves in the transition between target and antitarget patterns is introduced in Ref. [12]. The investigation of a model for cyclically competing species on a continuous space resulted in switches between spiral and plane-wave patterns [13]. Complex dynamics and spatiotemporal pattern formation in variant predator-prey models are analyzed in Refs. [14–17]. Study of self-organizing patterns maintained by competing associations in a six-species predator-prey model is proposed in Ref. [18].

One of the promising applications of the phenomenon of pattern formation could be digital image processing when the evolving pattern would be used to encode the initial image. A digital fingerprint image is used as the initial condition for the evolution of a pattern in a model of reaction-diffusion cellular automata [19], though the possibility of encrypting the initial fingerprint in the evolved pattern is not discussed in Ref. [19].

The main goal of this paper is to propose a secure steganographic communication algorithm based on the evolution of self-organizing patterns. In general, cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process [20]. Modern cryptography follows a strongly scientific approach and designs cryptographic algorithms around computational hardness assumptions that are assumed hard to break by an adversary. But cryptography does not always provide safe communication.

Steganography is a science of concealing data in a communication in such a way that only the sender and receiver know of its existence [21]. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties [22]. As mentioned previously, we will demonstrate that self-organizing patterns can be effectively exploited as a secure tool for steganographic communication.

[*]Loreta.Saunoriene@ktu.lt
[†]Minvydas.Ragulskis@ktu.lt; www.personalas.ktu.lt/∼mragul/

II. THE MODEL OF THE SYSTEM

We will exploit a well-known Beddington-DeAngelis-type predator-prey model with self- and cross-diffusion [14]. Governing equations of this model read:

$$\begin{aligned}\frac{\partial N}{\partial t} &= r\left(1-\frac{N}{K}\right)N - \frac{\beta N}{B+N+wP}P \\ &\quad + D_{11}\nabla^2 N + D_{12}\nabla^2 P, \\ \frac{\partial P}{\partial t} &= \frac{\varepsilon\beta N}{B+N+wP}P - \eta P + D_{21}\nabla^2 N + D_{22}\nabla^2 P,\end{aligned} \tag{1}$$

where t denotes time; N and P are densities of preys and predators, respectively; β is a maximum consumption rate, B is a saturation constant; w is a predator interference parameter ($w<0$ represents the case where predators benefit from cofeeding); η represents a per capita predator death rate; and ε is the conversion efficiency of food into offspring. It can be noted that the term $r(1-\frac{N}{K})$ characterizes the growth rate of preys; $\frac{\beta N}{B+N+wP}$ represents the functional response (the consumption rate of preys by an average single predator). The operator $\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$ is the Laplacian operator in the two-dimensional space. Self-diffusion terms $D_{11}\nabla^2 N$ and $D_{22}\nabla^2 P$ imply the movements of individuals from a higher to lower concentration region. Self-diffusion coefficients are denoted by D_{11} and D_{22}, respectively. $D_{12}\nabla^2 P$ and $D_{21}\nabla^2 N$ are cross-diffusion terms that biologically imply the countertransport. The cross-diffusion coefficient D_{12} represents the tendency of preys to keep away from predators. D_{21} represents the tendency of a predator to chase its prey. The cross-diffusion coefficients may be positive (which then denotes the tendency of one species to move in the direction of a lower concentration of another species) and negative (which then expresses the population fluxes of one species in the direction of higher concentration of another species) [14].

Nonzero initial conditions

$$N(x,y,0) > 0; \quad P(x,y,0) > 0 \tag{2}$$

are set in a rectangular domain $(x,y) \in \Omega = [0,L_x] \times [0,L_y]$, where L_x and L_y are the size of the system in the directions of x and y axis. Neumann, or zero-flux, conditions are set on the boundary:

$$\frac{\partial N}{\partial n} = \frac{\partial P}{\partial n} = 0; \quad (x,y) \in \partial\Omega, \tag{3}$$

where n is the outward unit normal vector of the smooth boundary $\partial\Omega$. Zero-flux boundary conditions imply that no external input is imposed from outside.

A. Equilibrium points

In the absence of diffusion, the model has three equilibria in the positive quadrant [14]:

(1) $(0,0)$ (total extinct) is a saddle point.

(2) $(K,0)$ (extinct of predators or preys-only) is a stable node if $\varepsilon\beta < \eta$ or $\varepsilon\beta > \eta$ and $K < -\frac{\eta B}{-\varepsilon\beta+\eta}$; a saddle if $\varepsilon\beta < \eta$ and $K > -\frac{\eta B}{-\varepsilon\beta+\eta}$; a saddle node if $\varepsilon\beta < \eta$ and $K = -\frac{\eta B}{-\varepsilon\beta+\eta}$.

(3) A nontrivial stationary state (N^*,P^*) (coexistence of preys and predators), where

$$\begin{aligned}N^* &= \frac{1}{2rw\varepsilon}K(rw\varepsilon - \varepsilon\beta + \eta) \\ &\quad + \frac{1}{2rw\varepsilon}\sqrt{K^2(rw\varepsilon-\varepsilon\beta+\eta)^2 + 4rKw\varepsilon\eta B}, \\ P^* &= \frac{(\beta\varepsilon-\eta)}{w\eta}N^* - \frac{B}{w}.\end{aligned} \tag{4}$$

B. The Turing instability

Governing equations (1) can be linearized assuming small perturbations around the stationary state (N^*,P^*): $N = N^* + \widetilde{N}$ and $P = P^* + \widetilde{P}$, where $|\widetilde{N}|, |\widetilde{P}| \ll 1$. The linearized form of the model reads

$$\begin{aligned}\frac{\partial \widetilde{N}}{\partial t} &= J_{11}\widetilde{N} + J_{12}\widetilde{P} + D_{11}\nabla^2\widetilde{N} + D_{12}\nabla^2\widetilde{P}, \\ \frac{\partial \widetilde{P}}{\partial t} &= J_{21}\widetilde{N} + J_{22}\widetilde{P} + D_{21}\nabla^2\widetilde{N} + D_{22}\nabla^2\widetilde{P},\end{aligned} \tag{5}$$

where coefficients $J_{kl}, (k,l = 1,2)$ are explicitly derived in Ref. [14]. Application of Routh-Hurwitz criteria for the solution to the linear model (5) helps to derive the necessary condition for the equilibrium point being locally asymptotically stable, the condition of the diffusion instability, and the criterion of Turing instability, which reads [14]

$$D_{11}J_{22} - D_{12}J_{21} - D_{21}J_{12} + D_{22}J_{11} > 2\sqrt{\det(D)\det(J)},$$

where $D = \left[\begin{smallmatrix} D_{11} & D_{12} \\ D_{21} & D_{22}\end{smallmatrix}\right]$; $J = \left[\begin{smallmatrix} J_{11} & J_{12} \\ J_{21} & J_{22}\end{smallmatrix}\right]$.

C. The numerical model and types of self-organizing patterns

A standard five-point approximation for a two-dimensional Laplacian with the zero-flux boundary conditions is used. The concentrations $(N_{ij}^{n+1}, P_{ij}^{n+1})$ at the moment $(n+1)\tau$ at mesh position (x_i, y_j) are calculated as [14]

$$\begin{aligned}N_{ij}^{n+1} &= N_{ij}^n + \tau D_{11}\Delta_h N_{ij}^n + \tau D_{12}\Delta_h N_{ij}^n + \tau f\left(N_{ij}^n, P_{ij}^n\right), \\ P_{ij}^{n+1} &= P_{ij}^n + \tau D_{21}\Delta_h N_{ij}^n + \tau D_{22}\Delta_h P_{ij}^n + \tau g\left(N_{ij}^n, P_{ij}^n\right),\end{aligned} \tag{6}$$

where the Laplacian is

$$\Delta_h N_{ij}^n = \frac{N_{i+1,j}^n + N_{i-1,j}^n + N_{i,j+1}^n + N_{i,j-1}^n - 4N_{i,j}^n}{h^2}.$$

Initially, the entire system is placed in the stationary state (N^*,P^*) with a random perturbation. The system evolves either into a steady or time-dependent state after a certain number of iterations. Different sets of the model parameters correspond to the special types of final patterns: the distinct stripelike patterns, a regular spotted pattern (hot or cold spots), the mixture of spotted and stripelike patterns, or the spiral wave patterns [14].

III. A SECURE COMMUNICATION SYSTEM BASED ON SELF-ORGANIZING PATTERNS

We consider a Beddington-DeAngelis-type predator-prey model with self- and cross-diffusion with the following parameter set: $D_{11} = 0.01, D_{12} = 0.0115, D_{21} = 0.01, D_{22} = 1,$

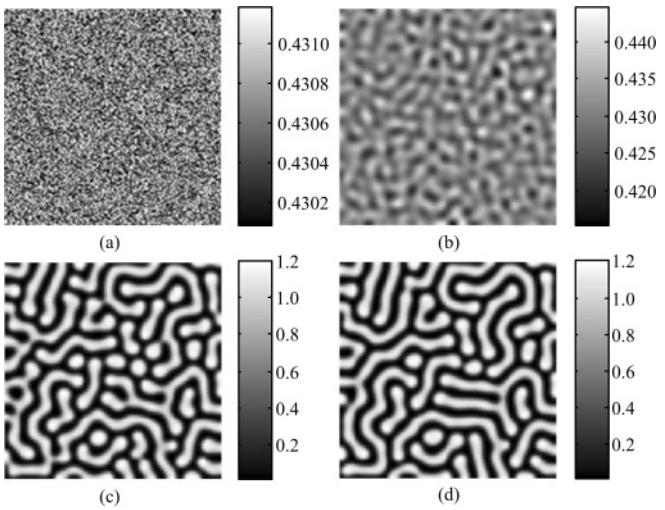

FIG. 1. Dynamics of the time evolution of preys: (a) the initial distribution ($\varepsilon = 10^{-3}$); (b) after 10 000 iterations; (c) after 50 000 iterations; (d) after 200 000 iterations.

$r = 0.5$, $\varepsilon = 1$, $\beta = 0.6$, $K = 2.6$, $\eta = 0.25$, $\omega = 0.4$, $B = 0.3154$. Numerical integration of differential equations (1) is performed with time step $\tau = 0.01$ and space step $h = 0.25$; the system size is 200×200 grayscale pixels ($L_x = L_y = 50$). Figure 1 demonstrates the dynamics of the time evolution of preys N. The stable equilibrium point ($N^* = 0.430\,58$; $P^* = 0.718\,555$) with small random perturbations is presented in Fig. 1(a). The logistic map

$$x_{i+1} = 4x_i(1 - x_i) \tag{7}$$

is used for the computation of a set of 200×200 pseudorandom numbers distributed in the interval $[0; 1]$. This random set is linearly transformed into an ε-length interval with zero mean before it is added to the initial concentration of preys:

$$[N]|_{t=0} = N^*[1] + [\widetilde{N}], \quad [P]|_{t=0} = P^*[1], \tag{8}$$

where $[1]$ is a 200×200 matrix of ones; $[\widetilde{N}]$ is a 200×200 matrix of pseudo-random numbers distributed uniformly in the interval $[-\varepsilon/2; \varepsilon/2]$. It is clear that the parameter ε must be significantly lower than the maximum concentrations in the final N and P patterns; we use $\varepsilon = 10^{-3}$ in computational experiments illustrated in Fig. 1.

Figures 1(b) and 1(c) show the evolution of the spatial pattern of preys after 10 000 and 50 000 iterations. A time-independent self-organizing pattern of stripes and spots is obtained after 200 000 iterations [Fig. 1(d)]. It is important to note that the pattern shown in Fig. 1(d) is sensitive to initial conditions. Figure 3(a) shows the initial distribution of preys, and Fig. 3(b) represents the pattern after 200 000 iterations (all parameters of the system are kept the same). Different initial perturbations in Eq. (8) (a different set of pseudorandom numbers) evolve into a pattern of the same type as shown in Fig. 3(d) but with a different writing.

A. The generation of target patterns

The fact that the evolution of self-organizing patterns is sensitive to initial perturbations allows construction and manipulation of target patterns by small modifications in the initial distribution of preys.

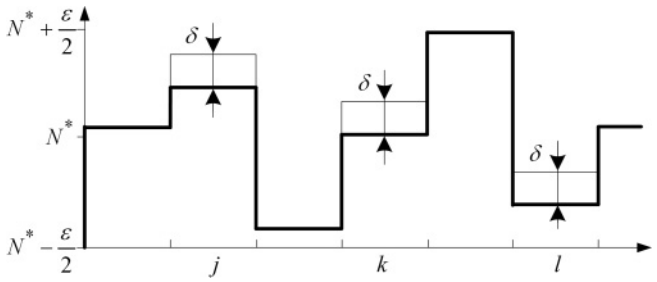

FIG. 2. The modification of the initial random density of preys. The thick solid line represents numerical values of pixels in a one-dimensional segment of the initial perturbation matrix $[\widetilde{N}]$. Thin solid lines represent concentrations of preys at pixels j, k, and l.

The sensitivity of the pattern evolution to initial conditions is supported in the creation of different defects (dislocations, dislinations, etc.), which are responsible for creating metastable equilibrium states [23]. These effects are illustrated in Figs. 1(d) and 3(b) and were two different realizations of initial concentrations of a preys result into apparently similar but locally different patterns of stripes.

Let us assume that the matrix of random perturbations $[\widetilde{N}]$ is modified by adding a positive constant δ to numerical values of some pixels in the initial distribution of preys. In general, the initial density of preys then can be described by the following equation:

$$[N]|_{t=0} = N^*[1] + [\widetilde{N}] + \delta[M], \tag{9}$$

where δ is a fixed constant; $[M]$ is a binary mask matrix holding ones at those pixels where the initial random density of the preys is increased by δ and zeros where the random density of preys is kept unchanged. Figure 2 illustrates a one-dimensional representation of the modification procedure of the initial random density of preys.

It is clear that different levels of δ would lead to the different patterns when the system evolves in time. The question if such a modification of the initial distribution of preys would evolve into an interpretable target pattern remains open.

Let us assume that the initial random density of preys [Fig. 3(a)] is changed by adding a T-shaped mask. Numerical values of pixels in the zone occupied by the letter T are incremented by δ; all other pixels remain unchanged. Figures 3(c), 3(e), and 3(g) represent modifications of the initial distribution of preys for different values of δ. It appears that the striped-spotted pattern of preys mimics the shape of the mask after 200 000 iterations if only δ was sufficiently high. It can be noted that a larger ratio δ/ε corresponds to a clearer target image in final patterns [Figs. 3(d), 3(f), and 3(h)]. Unfortunately, the ratio $\delta/\varepsilon = 0.1$ [Fig. 3(c)] does not yield an interpretable pattern [Fig. 3(d)]. But even such relatively small modifications in the initial distribution of preys are statistically detectable (the shape of the mask can be seen by a naked eye in Fig. 3(c). Therefore, such an approach cannot be considered as a safe technique for encoding secret information.

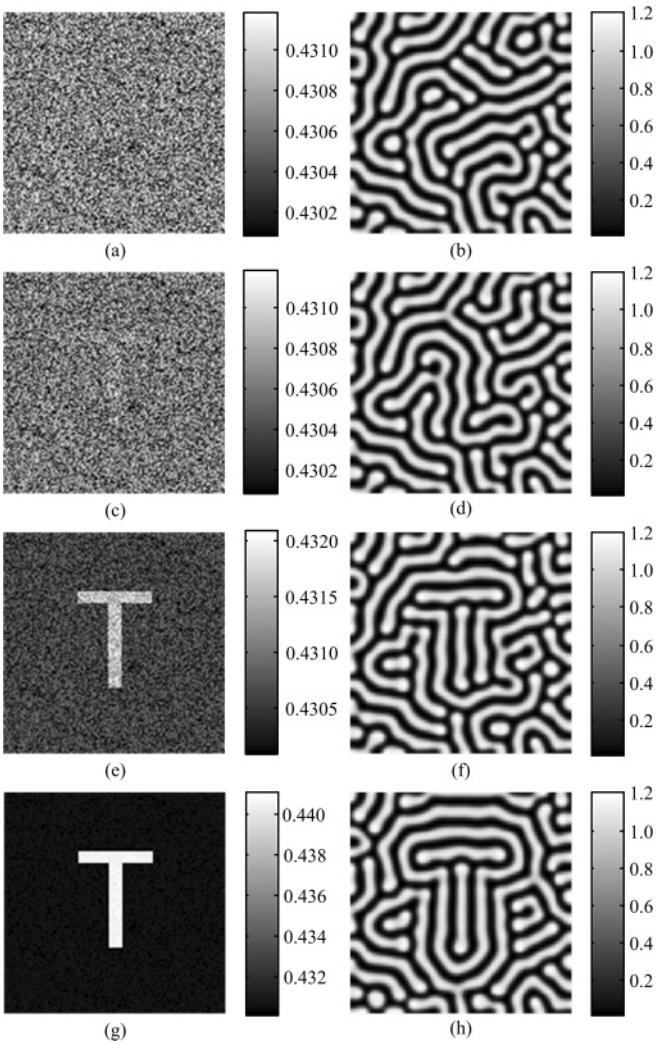

FIG. 3. Time evolution of preys: (a) the initial density of preys ($\varepsilon = 10^{-3}$; $\delta = 0$); (b) the pattern of preys after 200 000 iterations. Panels (c), (e), and (g) represent initial densities of preys distorted by the T-shaped mask at $\delta/\varepsilon = 0.1$, $\delta/\varepsilon = 1$, and $\delta/\varepsilon = 10$, respectively (the same matrix $[\widetilde{N}]$ is used in all experiments). Panels (d), (f), and (h) illustrate patterns of preys after 200 000 iterations.

B. A steganographic communication scheme based on the difference between evolving patterns

Previous computational experiments show that modifications of the initial random density of preys cannot be considered as a safe encoding of secret visual information: The target pattern becomes interpretable only when the initial distribution of preys reveals the secret to a naked eye. Therefore, we propose an encoding scheme based not on a target pattern but on the difference between two evolving patterns.

The first step of the procedure remains unchanged: We construct the initial random distribution of preys Eq. (8) and compute the density of preys after the system evolves m iterations in time [Figs. 1(a) and 1(b)]. The initial random distribution of preys must be perturbed in the next step. We use Eq. (9) for the perturbation, but the mask $[M]$ now holds not a target pattern but skeleton dots of the secret image instead

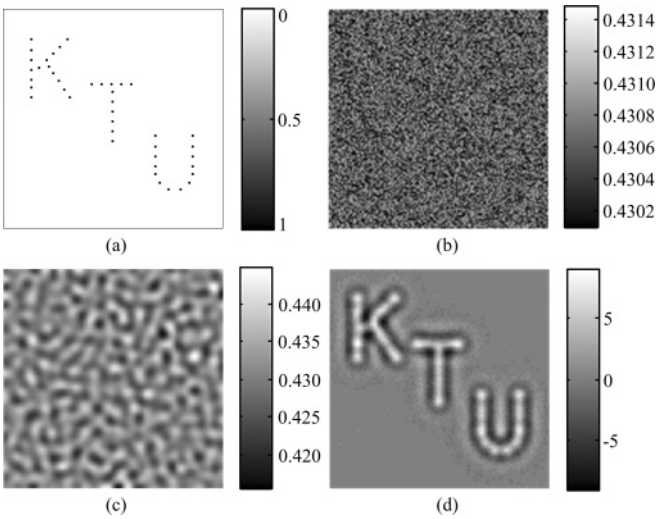

FIG. 4. A steganographic communication scheme based on the difference between evolving patterns. (a) The dot-skeleton representation of the secret image; (b) the perturbed initial distribution of preys; $\delta/\varepsilon = 0.3$; [the initial distribution of preys is shown in Fig. 1(a)]; (c) time evolution of (b) after 10 000 iterations; (d) the difference between panel (c) and Fig. 1(b).

[Fig. 4(a)]. It can be noted that the matrix $[\widetilde{N}]$ must be kept the same in both computational experiments and that δ is low enough to prevent statistical identification of the perturbation [we use $\delta/\varepsilon = 0.3$ in Fig. 4(b)]. Now, the density of preys is computed after the system evolves m iterations in time [Fig. 4(c)]. In fact, one could hardly see any differences between Fig. 1(b) and Fig. 4(c). Anyway, we compute the difference between these two patterns; the resulting image is shown in Fig. 4(d). It can be noted that the color bar in Fig. 4(d) shows the difference in pixel levels (grayscale levels are measured in the interval [0; 255]), while color bars in Figs. 4(b) and 4(c) show actual concentration of preys.

The secure communication system based on the formation of self-organizing patterns can be described by the following steps.

(1) The encoding process:
(a) Define the initial condition $0 < x_0 < 1$ ($x_0 \neq 3/4$); the number of time steps m; values of parameters ε and δ.
(b) Use the logistic map Eq. (7) to generate the set of pseudorandom numbers distributed in the interval [0; 1].
(c) Use Eq. (8) to generate initial densities of predators and preys.
(d) Generate the dot-skeleton representation of the secret image and construct the mask matrix $[M]$.
(e) Use Eq. (9) to perturb initial densities of preys.
(f) Use the numerical scheme Eq. (6) for m time steps and save the digital image of the evolved pattern.
(2) Send the encoded information to the receiver:
(a) Send the saved image of the pattern.
(b) Send the key x_0 (m, ε, and δ are fixed beforehand).
(3) Decoding the secret:
(a) Set the initial condition x_0 and use Eq. (7) to generate the set of pseudorandom numbers.
(b) Use Eq. (8) to generate initial distributions of predators and preys.

(c) Use the numerical scheme Eq. (6) for m time steps and save the digital image of the self-organizing pattern.
(d) The difference between the computed pattern and the received pattern reveals the secret image.

In principle, the necessity to send the key x_0 to the receiver (he or she needs x_0 to generate the unmodified initial conditions) could be avoided. The grayscale level (a whole number from the interval [0,255]) of a preselected pixel in the pattern evolved from the modified initial distribution of preys could be used to conceal the value of x_0. The sender could select x_0 freely from the set $\{0; 1/255; 2/255; \ldots; 1\}$ and place x_0 at the top left corner of the unmodified initial conditions. The dot-skeleton representation should be placed as far as possible from the top left corner then. The number of time steps m should be kept in a range that does not allow the evolving perturbation to reach the top left corner (the evolution of patterns in the area around the top left corner should be identical in the perturbed and the unperturbed images). The receiver then can divide the grayscale level of the top left pixel in the perturbed pattern by 255 and generate the unmodified initial conditions.

Of course, more sophisticated schemes for concealing the value of x_0 in the perturbed pattern could be exploited, but that is left as a definite subject for future research. This is somewhat similar to the normal Rivest, Shamir and Adleman (RSA) scheme [24], where the problem of distributing the keys has been suppressed. Nevertheless, the proposed communication algorithm possesses a definite advantage over the RSA scheme as it allows the possibility to conceal the fact that some secret information is buried in the exchanged pattern.

IV. ADVANTAGES AND LIMITATIONS OF THE PROPOSED COMMUNICATION SCHEME

As mentioned previously, steganography includes the concealment of information within computer files. Steganographic coding may be present inside of a transport layer, such as a document file, image file, program, or protocol. Our approach could be classified as a variant of text steganography inside a cover image. Various algorithms have been proposed to implement steganography in digital images. They can be categorized into three major clusters: algorithms using the spatial domain such as S-Tools [25], algorithms using the transform domain such as F5 [26] and algorithms taking an adaptive approach combined with one of the former two methods, e.g., ABCDE (A Block-based Complexity Data Embedding) [27]. Most of the existing steganographic methods rely on two factors: the secret key and the robustness of the algorithm.

A number of different methods exist to utilize the concept of steganography. Least significant bit (LSB) insertion is a common and simple approach to embed secret text information in a cover object. Three bits in each pixel can be stored by modifying the LSBs of the R, G, and B array in a 24-bit image as cover. To the human eye, the resulting stego image will look identical to the cover image [28,29]. The LSB modification concept can be used to hide data in an image. Each pixel is modified sequentially in the scan lines across the image; the portion where the secret message is hidden is degraded while the rest remain untouched [29,30]. A random LSB insertion method is developed in Ref. [31], where the secret data are spread out among the cover image in a seemingly random diffused manner. The key is used to generate pseudorandom numbers, which identify where, and in what order, the hidden message is laid out. An LSB insertion steganographic method coupled with high-security digital layers is proposed in Ref. [32]. Such encryption strategy makes it difficult to break through the encryption of the secret data and confuse steganalysis. A heuristic approach to hide data using LSB steganography technique is proposed in Ref. [33]. The secret data are encoded and afterwards hidden behind a cover image by modifying the least significant bits of each pixel of the cover image.

A definitive advantage of the proposed secret communication scheme is determined by the complexity of physical processes exploited in the encoding and decoding of secret visual information. The security of communicating parties is preserved since the transmittance of visual patterns does not attract the attention of eavesdroppers. In that respect our technique outperforms classical steganographic algorithms where some pixels of the cover image are modified in order to conceal a secret message in the cover image [21]. We transmit a smooth pattern that has evolved from perturbed initial conditions. It would be impossible to trace a perturbed pixel in the digital image of the evolved pattern.

On the other hand, the detection of perturbed pixels in the initial random distribution of preys (if the perturbed random initial distribution of preys would be transmitted instead of the evolved pattern) would be hardly possible. Skeleton points of the secret image are embedded into the random initial distribution of preys $[\widetilde{N}]$. The numerical value of δ used to encode the secret image into $[\widetilde{N}]$ is lower than the noise level [$\delta = 0.3\varepsilon$ in Fig. 4(b)]. Thus a straightforward identification of those secret skeleton dots is hardly possible from the statistical point of view.

A. The storage capacity of secret information

A characteristic feature of any secret communication scheme is the storage capacity of secret information. The quantity of information (the cover image) required to encrypt the secret using our technique is quite high compared to other digital encryption techniques [21]. Conventional steganographic techniques enable a straightforward embedding of a secret digital image and/or text into the cover image [21]. A number of special manipulations with pixels of the cover image are necessary to conceal the secret.

A definitive limitation of our technique is the fact that the encoded secret must be represented in a form of stripes. In general, the storage capacity of secret information for our technique is limited by the average width of stripes in the dynamically evolving pattern. The proposed technique cannot be used to encode symbols smaller than the average width of a stripe. This limitation is illustrated in Figs. 5 and 6. We use the same parameters of the system but modify the matrix $[M]$; it holds only two skeleton dots now. The distance between those two skeleton dots is gradually decreased until two separate highlighted zones merge into one region in the difference image. The clearance between two skeleton dots is 20 pixels in Fig. 5(a), 15 pixels in Fig. 5(b), 10 pixels in Fig. 5(c), and 7

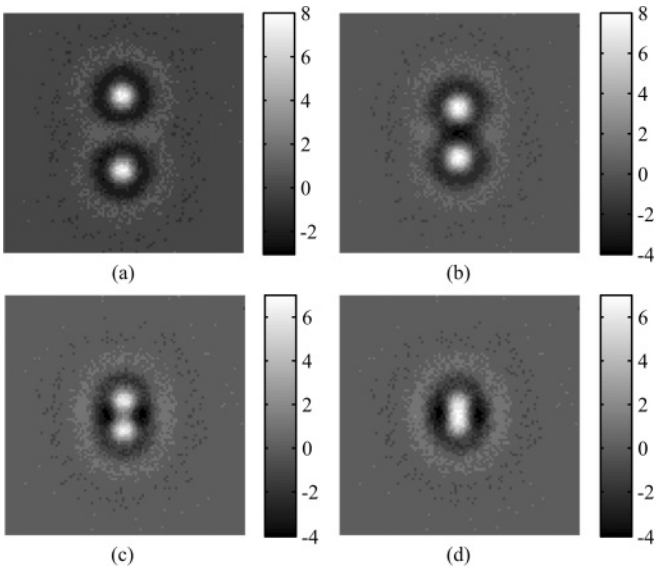

FIG. 5. The development of a stripe between two dots in the difference image: (a) the clearance between two skeleton dots is 20 pixels; (b) 15 pixels; (c) 10 pixels; (d) 7 pixels.

pixels in Fig. 5(d) (color bars show the difference in grayscale levels). Thus, a clearance of 7 pixels between two adjacent pixels ensures the development of a well-interpretable stripe in the difference image. Another important feature determining the storage capacity of secret information is the minimum distance between two stripes. Two separate stripes can be clearly interpreted in the difference image when the distance between the center lines of the stripes is 20 pixels [Fig. 6(a)]. It can be noted that every stripe is composed from 7 skeleton dots; the distance between adjacent skeleton dots is 7 pixels. Two separate stripes can be still interpreted in Figs. 6(b) and 6(c), but both stripes almost merge together when the distance between the center lines becomes equal to 7 pixels

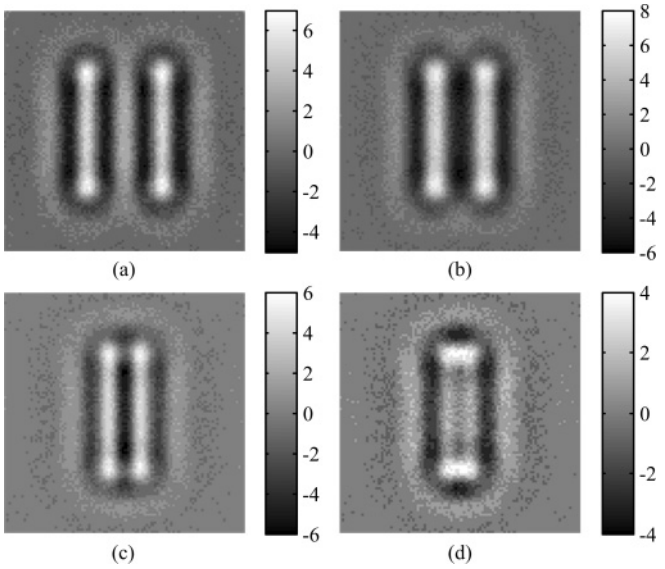

FIG. 6. The mingling of two separate stripes in the difference image: (a) the clearance between two parallel stripes is 20 pixels; (b) 15 pixels; (c) 10 pixels; (d) 7 pixels.

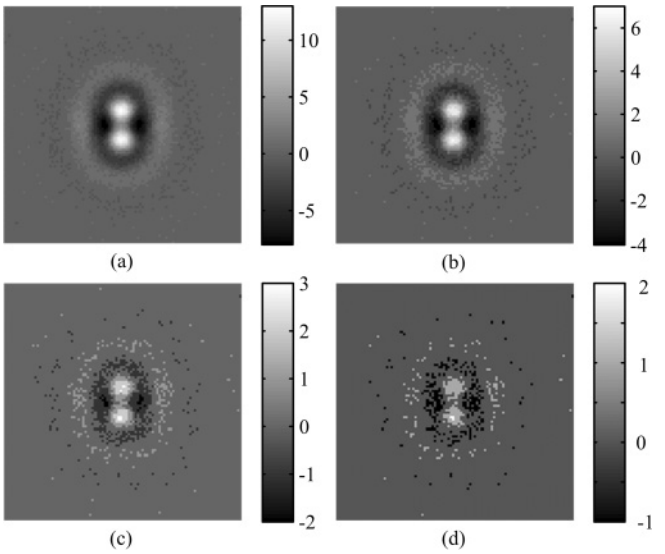

FIG. 7. The ratio δ/ε does not have a noticeable influence to the shape of the developing stripe: (a) $\delta/\varepsilon = 0.1$; (b) $\delta/\varepsilon = 0.2$; (c) $\delta/\varepsilon = 0.5$; (d) $\delta/\varepsilon = 1$ ($\varepsilon = 10^{-3}$ in all computational experiments).

[Fig. 6(d)]. Finally, it can be noticed that the ratio δ/ε does not have a noticeable influence to the shape of the developing stripe in the difference image, though the clarity of the image, of course, depends on this ratio (Fig. 7).

The functionality of the proposed technique is demonstrated using a computational example illustrated in Fig. 8. The secret image is shown in Fig. 8(a); its dot-skeleton representation in Fig. 8(b) (the distance between dots in the direction of the x and y axis is 7 pixels). The encrypted image is shown in Fig. 8(c); the evolved pattern from the encrypted image (after 10 000 iterations) is shown in Fig. 8(d). The evolved pattern from the random perturbation (without the embedded dot-skeleton representation of the secret image) is shown in Fig. 8(e). The difference between Fig. 8(d) and Fig. 8(e) is shown in Fig. 8(f).

A naked eye cannot see any differences between Figs. 8(d) and 8(e). But it is important to note that the actual difference between Figs. 8(d) and 8(e) is a smooth image; the secret information is not hidden at some isolated pixels. Steganalysis procedures [34] would not be able to detect the fact that some secret information is being transmitted by means of Fig. 8(d).

B. The propagation of the initial perturbation through iterations

As mentioned previously, the main idea of the proposed method exploits the fact that slight modifications of the initial conditions result in slight modifications in the evolved pattern. The subtraction of the unmodified pattern from the modified one enables to recover the secret modification. The propagation of modifications through iterations is an important factor determining the effective range of m where the proposed communication algorithm is applicable.

We use Eq. (8) to generate initial densities of predators and preys, let the system evolve for m time steps, and save the digital image of the evolved pattern. Next, we repeat the

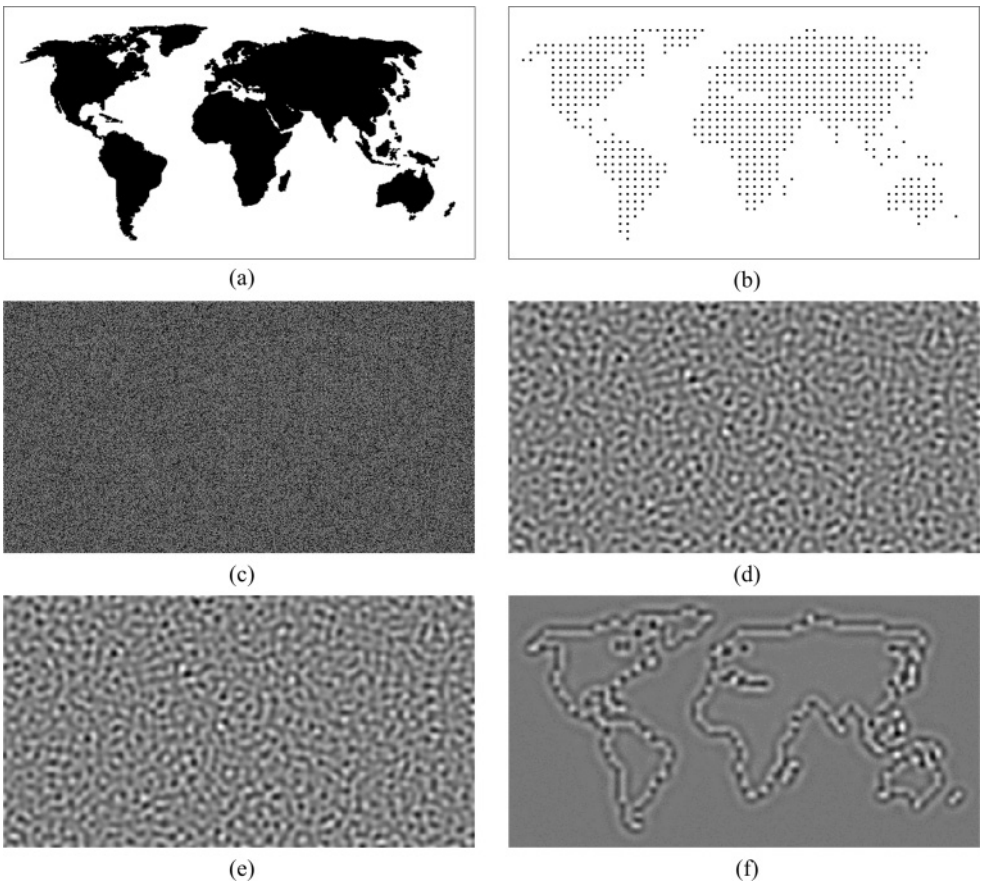

FIG. 8. The illustration of steganographic visual communication system based on self-organizing patterns: (a) the secret image; (b) the dot-skeleton representation of the secret image; (c) the random initial distribution of preys with the embedded dot-skeleton representation of the secret image; (d) time evolution of (c) after 10 000 iterations; (e) time evolution of the random initial distribution of preys without the embedded dot-skeleton representation of the secret image; (f) the difference between panels (d) and (e) reveals the secret image.

computational experiment but use Eq. (9) to perturb initial densities of preys (the mask matrix $[M]$ is the same as in Fig. 4) and let the system evolve for m time steps again (m is the same as before). Now, the difference between two digital images is assessed by computing the root-mean-square error E of the difference:

$$E(m) = \frac{1}{200^2}\sqrt{\sum_{k=1}^{200}\sum_{l=1}^{200}(N_{kl}|_{t=m\tau} - M_{kl}|_{t=m\tau})^2}, \quad (10)$$

where N_{kl} is the concentration of preys in the evolved pattern at the k row and l column; M_{kl} is the concentration of preys in the initially perturbed pattern at the k row and l column. We repeat computational experiments for different m; the results are presented in Fig. 9.

It is clear that $E(0)$ is quite low: The initial density of preys is perturbed only at several pixels. It is interesting to observe that E becomes smaller when the system starts to evolve. It can be explained by the fact that initial perturbations diffuse among the nearest pixels surrounding the dot-skeleton representation of the secret image at small m. But complex pattern formation processes start to dominate as the number of time steps increases. E of the difference between two digital images reaches the initial level at around 4500 time steps (at $\delta/\varepsilon = 0.3$) and then continues increasing almost at an exponential law. It can be noted that $E(m)$ is measured not in grayscale levels but in concentrations of preys at appropriate nodes. In general, differences between two evolved patterns are very small in average even after 10 000 time steps. Nevertheless, majority of changes in the self-organizing pattern are grouped around the dot-skeleton representation of the secret image then. This fact enables visual interpretation

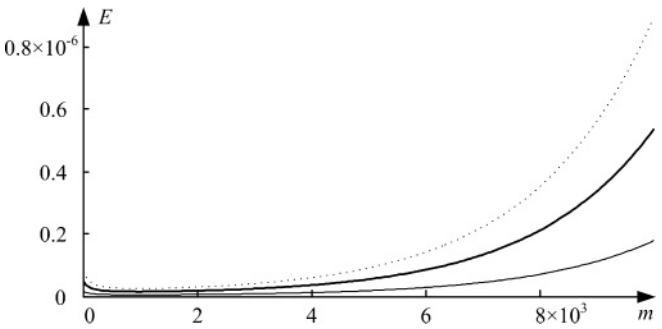

FIG. 9. E of the difference between patterns evolved from the initial and the perturbed densities of preys at different m (note that E is computed in actual concentrations of preys, not in grayscale levels at corresponding pixels). The dotted line stands for $\delta/\varepsilon = 0.5$; the thick solid line – $\delta/\varepsilon = 0.3$; the thin solid line – $\delta/\varepsilon = 0.1$.

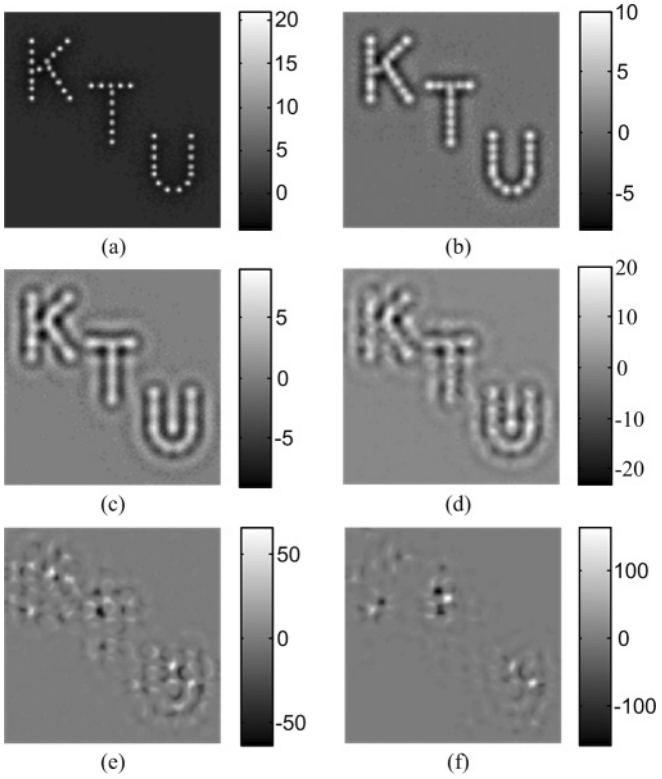

FIG. 10. The evolution of the difference pattern at $\delta/\varepsilon = 0.3$: (a) $m = 1000$ iterations; (b) 5000 iterations; (c) 15 000 iterations; (d) 20 000 iterations; (e) 25 000 iterations; (f) 40 000 iterations.

of the secret information in the difference image [Fig. 4(d)]. Further increase of the number of time steps enlarges the E but differences get diffused throughout the image and it becomes difficult to interpret the secret already at $m = 25\,000$.

The evolution of the difference pattern is illustrated in Fig. 10. Initially (until m is small) differences are visible only around the dot-skeleton points [Fig. 10(a)]. But perturbations quickly diffuse around the dot-skeleton representation of the secret image [Figs. 10(b)–10(d)]. Complex pattern formation processes deform the perturbed pattern so much at high m (in the global domain) that visual interpretation of the secret image becomes impossible [Figs. 10(e) and 10(f)]. Note that all differences are measured in grayscale levels.

It is clear that the iteration number m becomes an important system parameter due to complex pattern formation processes. Another important question is about the sensitivity of the decoding procedure of the proposed scheme to the iteration number m. The recipient of the perturbed pattern must generate the unperturbed pattern before the secret can be revealed by subtracting these too patterns. It is important to assess the robustness of the proposed scheme if the recipient is able to generate the correct initial distribution of preys but uses wrong number of time steps $n \neq m$ to evolve the unperturbed pattern.

In general, this is a nontrivial digital pattern recognition problem [35]. The interpretation of the secret image becomes a complex problem when iteration numbers used to generate the perturbed and the unperturbed patterns are different. We propose a straightforward method for the assessment of the quality of the secret text in the difference image: every

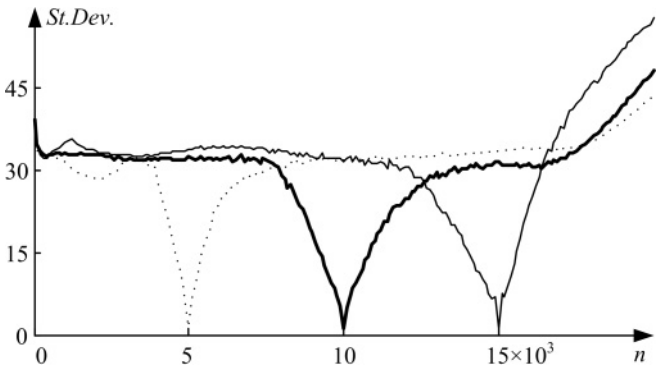

FIG. 11. The standard deviation of grayscale levels at the background around the dot-skeleton representation of the secret image; n stands for the number of time steps used to evolve the unperturbed pattern. The dotted line stands for $m = 5000$; the thick solid line for $m = 10\,000$; the thin solid line for $m = 15\,000$. Note that the standard deviation is calculated in the difference image.

pixel of the dot-skeleton representation of the secret image is surrounded by a circle whose radius is 25 pixels. This is a much larger distance than the optimal distance ensuring the development of a stripe between two dots in the difference image (Fig. 5). All pixels outside these zones are considered as the background. Now, we compute the standard deviation of grayscale levels of all pixels in the background and plot its variation in respect to n at fixed m (Fig. 11).

It can be seen that the standard deviation of grayscale levels of pixels in the background vanishes to 0 when $n = m$ (Fig. 11), which ensures the best interpretation of the secret text in the difference image. Sharp minimums in the surrounding of m denote high sensitivity of the proposed scheme to the selection of the correct number of time steps. It can be noted that visual interpretation of the secret information becomes impossible when the standard deviation in the background reaches 15 grayscale levels. The unsmooth variation of the standard deviation in Fig. 11 can be explained by the pixelization procedure, which rounds actual concentrations of preys to grayscale levels.

Now, let (N^*, P^*) is a stationary of the system described by Eq. (1). The Turing stability of this state is analyzed by linearizing small perturbations $N(t,x,y)|_{t=0} = N^* + \widetilde{N}(x,y)$ and $P(t,x,y)|_{t=0} = P^* + \widetilde{P}(x,y)$ around the stationary state; the resulting linear system for the determination of the evolution of $\widetilde{N}$ and $\widetilde{P}$ is described by Eq. (5). The hiding of the secret in the initial perturbation can be described as $N(t,x,y)|_{t=0} = N^* + \widetilde{N}(x,y) + \widetilde{\widetilde{N}}(x,y)$ and $P(t,x,y)|_{t=0} = P^* + \widetilde{P}(x,y) + \widetilde{\widetilde{P}}(x,y)$, where $\widetilde{\widetilde{N}}(x,y) = \widetilde{\widetilde{P}}(x,y) = 0$ almost everywhere except several points corresponding to the dot-skeleton representation of the secret image. Let (x_d, y_d) be a point in the dot-skeleton representation; $d = 1,2,\ldots,k$; where k is the number of points in the dot-skeleton representation. Note that $|\widetilde{\widetilde{N}}(x_d,y_d)| < |\widetilde{N}(x_d,y_d)|$; $|\widetilde{\widetilde{P}}(x_d,y_d)| < |\widetilde{P}(x_d,y_d)|$; $d = 1,2,\ldots,k$.

The evolution of $\widetilde{\widetilde{N}}$ and $\widetilde{\widetilde{P}}$ can be investigated using the linearized system described by Eq. (5) where $\widetilde{N}$ is replaced by $\widetilde{\widetilde{N}}$ and $\widetilde{P}$ is replaced by $\widetilde{\widetilde{P}}$. This is possible due to the principle of superposition, which holds for linear systems. Note that

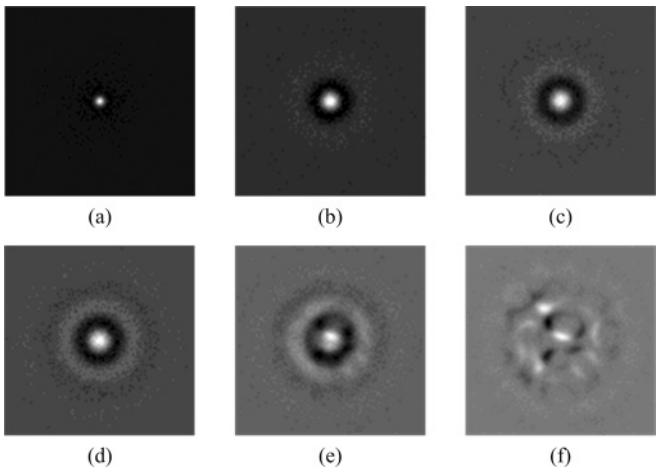

FIG. 12. The evolution of a single-dot type perturbation can be approximated by a linear model. The evolution of $\widetilde{\widetilde{N}}$ at (a) $m =$ 1000 iterations; (b) 5000 iterations; (c) 10 000 iterations; (d) 15 000 iterations; (e) 20 000 iterations; (f) 25 000 iterations ($\delta/\varepsilon = 0.3$).

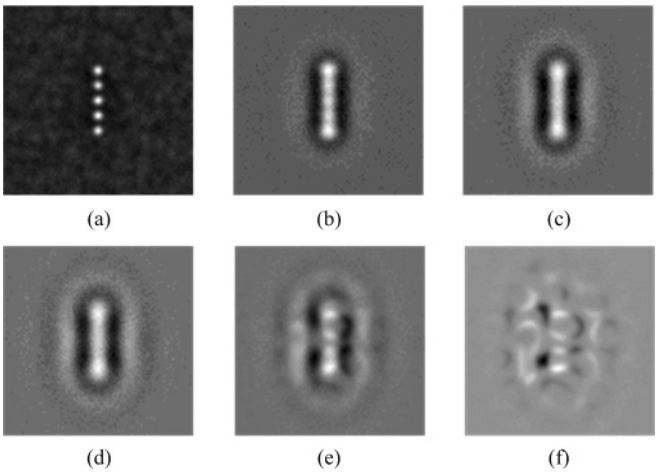

FIG. 13. The evolution of a multidot-type perturbation cannot be approximated by a linear model. The evolution of a stripe interconnecting five dot-skeleton points is illustrated at (a) $m =$ 1000 iterations; (b) 5000 iterations; (c) 10 000 iterations; (d) 15 000 iterations; (e) 20 000 iterations; (f) 25 000 iterations ($\delta/\varepsilon = 0.3$).

$\widetilde{\widetilde{N}}(t,x,y)|_{t=0} = \widetilde{\widetilde{P}}(t,x,y)|_{t=0} = 0$ almost everywhere except the points (x_d, y_d); $d = 1,2,\ldots,k$.

Proposition 1. Let (N^*, P^*) be the Turing unstable stationary point for a Beddington-DeAngelis-type predator-prey model with self- and cross-diffusion. Then the evolution of the dot-skeleton representation of the secret $[\widetilde{\widetilde{N}}(t,x,y); \widetilde{\widetilde{P}}(t,x,y)]$ through iterations cannot be described by a linear model.

We will prove Proposition 1 by contradiction using computational tools. Let us consider the situation when $k = 1$. The evolution of $\widetilde{\widetilde{N}}$ is shown in Fig. 12. It can be seen that linear diffusion processes dominate the evolution until $m = 20\,000$ where the clarity of the image is lost. Nevertheless, a linear model can be considered as a perfect approximation of transient processes in the interval $0 \leqslant m \leqslant 20\,000$.

Now we will consider a dot-skeleton representation consisting of 5 points grouped in a column. Let as assume that the linear model approximates the evolution of $\widetilde{\widetilde{N}}$ and $\widetilde{\widetilde{P}}$ in the interval $0 \leqslant m \leqslant 20\,000$. Then, according to the principle of superposition, five propagating rings of diffusion should be simply superposed at increasing m. Results of the computational experiments are illustrated in Fig. 13. The development of a stripe interconnecting the dot-skeleton points can be clearly seen in already at $m = 5000$ (note that the region surrounding the stripe is not altered much). This contradicts to the assumption that a linear model governs the evolution of the initial perturbation.

Complex pattern formation processes based on the Turing instability govern the formation of stripes interconnecting dot-skeleton points. On the other hand, the pattern of stripes modulated on top of the pattern evolved from the perturbed initial state can be detected by subtracting it from the pattern evolved from the unperturbed initial state. This effect can be considered as a simple linear superposition. Nevertheless, the formation of stripes representing the secret information is governed by complex nonlinear processes, and the interpretation of this secret pattern in the difference image is possible only due to the fact that the initial perturbation $\widetilde{\widetilde{N}}$ and $\widetilde{\widetilde{P}}$ is equal to zero almost everywhere.

C. Considerations about the type of the noise used to generate the initial concentration of preys

So far we have exploited the logistic map to generate the set of pseudorandom numbers for the perturbation of the initial distribution of preys around the stationary state N^*. One of the main reasons for the selection of the logistic map is the simplicity of the map and the fact that the properties of this map are well and thoroughly explored. But the most important reason in favor of the logistic map is the ability to minimize the length of the key. We do not transmit the initial unperturbed distribution of preys to the receiver: We do transmit only the initial condition x_0 (the receiver generates the distribution himself).

Nevertheless, it is important to investigate how other types of noise could affect the encryption of information. For example, dichotomous noise appears in a wide variety of physical and mathematical models where the symmetric dichotomous Markov process takes on the values ± 1 [36]. The implementation of such a dichotomous process fits well into the proposed scheme of communication. The only modification is performed in the generation of the matrix $[\widetilde{N}]$ [Eq. (8)]; every element of this matrix $\widetilde{n}_{kl}$ is now computed using the relationship:

$$\widetilde{n}_{kl} = \frac{\varepsilon}{2}\mathrm{sign}(x_i - 0.5), \tag{11}$$

where indexes k and l run consecutively in accordance to the iteration number i. Note that it is still sufficient to transmit the initial condition x_0. We repeat computational experiments with the dot-skeleton representation of the secret image used in Fig. 4 and keep other parameters unchanged. The perturbed symmetric dichotomous Markov process is shown

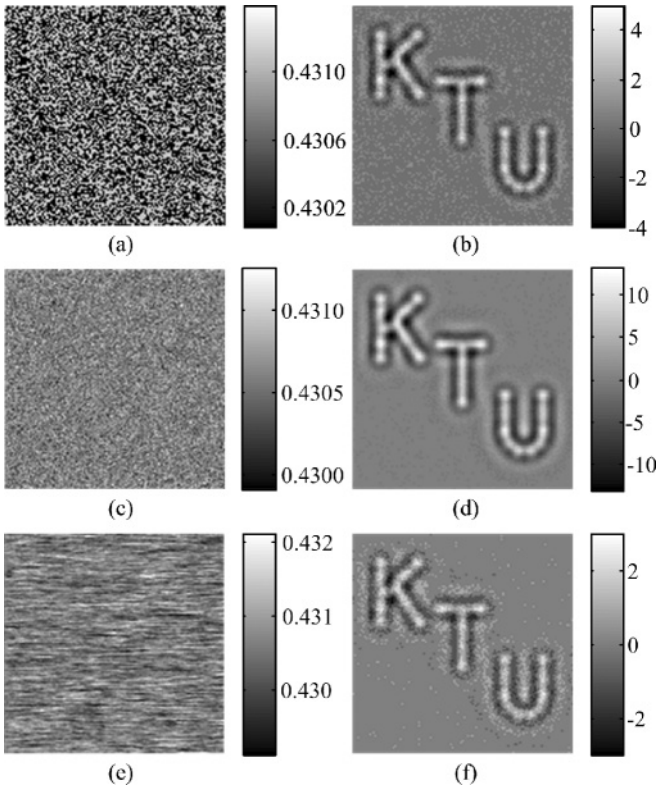

FIG. 14. Different types of noise affect the encryption of information: (a) and (b) the permuted initial distribution of preys and the secret image, respectively, in case of dichotomous noise; (c) and (d) normal noise; (e) and (f) colored noise.

in Fig. 14(a); $\delta/\varepsilon = 0.3$. It can be noted that it is possible to identify pixels of the dot-skeleton representation of the secret image in Fig. 14(a) (electronically or by a naked eye) due to the dichotomous distribution of pixels in the initial unperturbed stochastic distribution of preys. Nevertheless, this cannot be considered as a drawback of the system: The initial perturbed distribution of preys is not transmitted to the receiver, and it is impossible to trace the dot-skeleton representation of the secret in the evolved pattern. The difference between the patterns evolved from the perturbed and the unperturbed distributions of preys reveals the secret [Fig. 14(b)]. The secret image can be easily interpreted by a naked eye, but one can note a rather coarse graining at the background. It can be explained by the structure of the initial concentration of preys.

Analogous experiments are repeated with the Gaussian noise (the mean μ equal to 0 and the standard deviation σ equal to $\varepsilon/6$. We select $\sigma = \varepsilon/6$ because 99.73% of all generated points will fall into interval $[-\varepsilon/2; \varepsilon/2]$ according to the 3σ rule. The permuted initial distribution of preys ($\delta/\varepsilon = 0.3$) is shown in Fig. 14(c); the difference between the patterns evolved from the perturbed and the unperturbed distributions is shown in Fig. 14(d).

Finally, computational experiments are repeated with the colored noise, which can be generated by passing the white noise through a shaping filter [37]. We continue with the Gaussian noise [the mean equal to 0 and the standard equal to $\varepsilon/6$ and filter it by a low-pass filter by placing a pole near 1 at the unit circle and a zero at the origin; the syntax of the filtering operator in Matlab reads: $y =$ *filter(1,[1−0.9],randn(200*200,1)*]. The permuted initial distribution of preys ($\delta/\varepsilon = 0.3$) is shown in Fig. 14(e); the difference between the patterns evolved from the perturbed and the unperturbed distributions is shown in Fig. 14(f).

Comparisons between Fig. 4(d) and Figs. 14(b), 14(d), and 14(f) allow us to conclude that the secret is best interpretable when the initial distribution of preys is uniform in the interval $[-\varepsilon/2; \varepsilon/2]$. Worst results are produced by the dichotomous noise (it can be explained by the fact that initial perturbations are maximal in the whole domain then). In any case the receiver must be able to generate an identical copy of the initial distribution of preys; thus the optimal selection is the uniform noise generated by the logistic map.

V. CONCLUDING REMARKS

A new steganographic communication scheme based on evolving patterns is proposed in this paper. So far, we have used the perturbed pattern of preys to hide the skeleton of the secret image. Such an encoding scheme would work equally well if the pattern of predators would be used instead.

We have exploited the well-known Beddington-DeAngelis-type predator-prey model with self and cross-diffusion for the generation of evolving patterns. The ability to encrypt images in a self-organizing pattern is based on the sensitivity to initial conditions in the evolution of this pattern. In principle any nonlinear physical model of evolving patterns in isotropic systems, that have as equilibrium stripe-like patterns (the reaction-diffusion model, the two-phase flow model, the model of competing species, the disordered plane wave model, etc.) could be used as the algorithm for the computation of evolving Turing's patterns. Thus the applicability of the proposed communication scheme is not limited by a specific physical model and is based on the sensitivity to initial conditions of Turing's patterns, which form by the combination of diffusion and other processes such as reaction or convection. We admit that simpler models than the Beddington-DeAngelis-type predator-prey model with self- and cross-diffusion could be used for the same purpose. The Swift-Hohenberg equation [38] could be an example of a physical model where self-organizing patterns of stripes develop in a model described by a single scalar function defined on the plane (at appropriately tuned parameters of the model). But a Beddington-DeAngelis-type predator-prey model with self- and cross-diffusion has an advantage from the point of view of the security of the encryption: The dot-skeleton representation can be encrypted into one of the two scalar functions defined on the plane. Moreover, some part of the secret image can be encrypted in the initial distribution of preys; another, in the initial distribution of predators. The pattern of preys would become the inverse of the pattern of predators in the long run, but interesting transient processes could be successfully exploited for secret communication (all these addition security measures are left for the future research).

The storage capacity of secret information is relatively small and is predetermined by the average width of stripes in the evolving pattern. Nevertheless, the ability of the

proposed scheme to hide information and to avoid suspicion outperforms traditional steganographic techniques if the security of communication is considered as a primary objective.

ACKNOWLEDGMENT

Partial financial support from the Lithuanian Science Council under project No. MIP-041/2011 is acknowledged.

[1] J. E. Pearson, Science **261**(5118), 189 (1993).
[2] M. Seul and D. Andelman, Science **267**(5197), 476 (1995).
[3] K. J. Lee, W. D. McCormick, Q. Ouyang, and H. L. Swinney, Science **261**(5118), 192 (1993).
[4] S. Kondo and T. Miura, Science **329**(5999), 1616 (2010).
[5] A. Yochelis and M. Sheintuch, Phys. Rev. E **80**, 056201 (2009).
[6] S. Sen, P. Ghosh, S. S. Riaz, and D. S. Ray, Phys. Rev. E **80**, 046212 (2009).
[7] C. M. Topaz and A. J. Catllá, Phys. Rev. E **81**, 026213 (2010).
[8] Z.-K. Gao, N.-D. Jin, W.-X. Wang, and Y.-C. Lai, Phys. Rev. E **82**, 016210 (2010).
[9] M. G. Clerc, D. Escaff, and V. M. Kenkre, Phys. Rev. E **82**, 036210 (2010).
[10] G. Wang, Q. Wang, P. He, S. Pullela, M. Marquez, and Z. Cheng, Phys. Rev. E **82**, 045201 (2010).
[11] O. Kuksenok, V. V. Yashin, and A. C. Balazs, Phys. Rev. E **80**, 056208 (2009).
[12] X. Yuan, X. Lu, H. Wang, and Q. Ouyang, Phys. Rev. E **80**, 066201 (2009).
[13] X. Ni, W.-X. Wang, Y.-C. Lai, and C. Grebogi, Phys. Rev. E **82**, 066211 (2010).
[14] W. Wang, Y. Lin, L. Zhang, F. Rao, and Y. Tan, Comm. Nonlin. Sci. Numer. Simulat. **16**, 2006 (2011).
[15] W. Wang, L. Zhang, H. Wang, and Z. Li, Ecol. Model. **221**(2), 131 (2010).
[16] M. R. Garvie and C. Trenchea, J. Biol. Dyn. **4**(6), 559 (2010).
[17] B. Dubey, N. Kumari, and R. K. Upadhyay, J. Appl. Math. Comput. **31**, 413 (2009).
[18] G. Szabó, A. Szolnoki, and I. Borsos, Phys. Rev. E **77**, 041919 (2008).
[19] Y. Suzuki, T. Takayama, I. N. Motoike, and T. Asai, Int. J. Unconv. Comput. **3**, 1 (2007).
[20] V. V. Yaschenko, *Cryptography: An Introduction* (American Mathematical Society, Providence, RI, 2002).
[21] N. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking: Attacks and Countermeasures* (Springer, Amsterdam, 2001).
[22] F. A. P. Petitcolas and S. Katzenbeisser, *Information Hiding Techniques for Steganography and Digital Watermarking* (Artech House Publishers, Boston, 2000).
[23] L. Pismen, *Patterns and Interfaces in Dissipative Dynamics* (Springer Series in Synergetics) (Springer, Berlin, 2006).
[24] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, FL, 1996).
[25] ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip.
[26] http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html.
[27] H. Hioki, in *Proceedings of Pacific Rim Workshop on Digital Steganography* (July 2002), p. 30.
[28] N. F. Johnson and S. Jajodia, Computer **31**, 26 (1998).
[29] S. Bandyopadhyay, D. Bhattacharyya, P. Das, S. Mukherjee, and D. Ganguly, in *International Conference on Contemporary Computing* (IC3) (August 2008), p. 106.
[30] K. M. Singh, S. B. Singh, and L. S. S. Singh, International Journal of Computer Science and Network Security **7**, 302 (2007).
[31] M. Sutaone and M. Khandare, in *International Conference on Wireless, Mobile and Multimedia Networks* (WMMN) (January 2008), p. 146.
[32] N. N. EL-Emam, J. Comput. Sci. **3**, 223 (2007).
[33] S. K. Bandyopadhyay, D. Bhattacharyya, P. Das, S. Mukherjee, and D. Ganguly, in *International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing* (SNPD) (August 2008), p. 490.
[34] H. Wang and S. Wang, Comm. ACM **47**, 76 (2004).
[35] K. Koutroumbas and S. Theodoridis, *Pattern Recognition,* 4th ed. (Academic Press, Boston, 2008).
[36] I. Bena, C. Van den Broeck, R. Kawai, and K. Lindenberg, Phys. Rev. E **66**, 045603 (2002).
[37] F. Moss and P. V. E. McClintock, *Noise in Nonlinear Dynamical Systems* (Cambridge University Press, Cambridge, UK, 2007).
[38] J. Swift and P. C. Hohenberg, Phys. Rev. A **15**, 319 (1977).