# A Secure Communication System Based on Self-organizing Patterns

Paulius Palevicius*, Loreta Saunoriene†, Minvydas Ragulskis‡
Research Group for Mathematical and Numerical Analysis of Dynamical Systems,
Kaunas University of Technology, Studentu 50–222, Kaunas LT–51368, Lithuania,
Email: *Paulius.Palevicius@ktu.lt, †Loreta.Saunoriene@ktu.lt, ‡Minvydas.Ragulskis@ktu.lt

***Abstract*—This paper proposes a secure steganographic communication algorithm based on the evolution of self-organizing patterns. The presented algorithm is a modification of a secure steganographic scheme, presented in our previous work [1]. Algorithm is based on the formation of self-organizing patterns in a Beddington-deAngelis-type predator-prey model with self-diffusion. Computational experiments show that the generation of interpretable target patterns cannot be considered as a safe encoding of secret visual information because the target pattern becomes interpretable only when the cover image (initial distribution of preys) leaks the secret to a naked eye. Therefore, we propose an alternative approach when the cover image represents the self-organizing pattern which has evolved from initial states perturbed using the dot-skeleton representation of the secret image. Such visual communication technique protects both the secret image and communicating parties.**

***Index Terms*—Visual steganography, self-organizing pattern, nonlinear evolution.**

## I. Introduction

The field of research on pattern formation modelled by reaction-diffusion systems, which provides a general theoretical framework for describing pattern formation in systems from variant disciplines including biology, chemistry, physics, etc., seems to be an increasingly interesting area. One of the classical numerical examples illustrating a variety of irregular spatiotemporal patterns comprises a simple reaction-diffusion model with finite amplitude perturbations [2]. 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 [3]. Patterns specifying dynamic behavior of chemoresponsive gels undergoing the Belousov-Zhabotinsky reaction are constructed in [4]. Pattern formation mechanisms of a reaction-diffusion-advection system, with one diffusivity, differential advection, and Robin boundary conditions of Danckwerts type, are investigated in [5]. Time-periodic forcing of spatially extended patterns near a Turing-Hopf bifurcation point is studied in [6]. 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 [7], though the possibility to encrypt the initial fingerprint in the evolved pattern is not discussed in [7]. The dynamic behavior of predator-prey model has long been and will also continue to be one of the dominant themes in both ecology and mathematical ecology due to its universal existence and importance. Complex dynamics and spatiotemporal pattern formation in variant predator-prey models are analyzed in [8], [9], [10], [11].

This paper proposes a secure steganographic communication algorithm based on the evolution of self-organizing patterns. The algorithm is a modification of a secure steganographic scheme, presented in our previous work [1].

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 [12]. 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 [13]. 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 [14].

As mentioned previously, we will demonstrate that self-organizing patterns can be effectively exploited as a secure tool for steganographic communication.

## II. The model of the system

We exploit a well known predator-prey model with Beddington-DeAngelis-type functional response with self-diffusion [8]. The system of differential equations describing the dynamics of this model can be written:

$$\begin{aligned}\frac{\partial N}{\partial t} &= r\left(1-\frac{N}{K}\right)N-\frac{\beta N}{B+N+wP}P+d_1\nabla^2 N,\\ \frac{\partial P}{\partial t} &= \frac{\varepsilon\beta N}{B+N+wP}P-\eta P+d_2\nabla^2 P,\end{aligned} \tag{1}$$

where $t$ denotes time; $N$ and $P$ are densities of preys and predators respectively; $\beta$ is a maximum consumption rate, $B$ is a saturation constant; $w$ is a predator interference parameter; $\eta$ represents a per capita predator death rate; $\varepsilon$ is the conversion efficiency of food into offspring. It can be noted, that the operator

$$\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \tag{2}$$

is the Laplacian operator in the two-dimensional space. Self-diffusion terms $d_1 \nabla^2 N$ and $d_2 \nabla^2 P$ imply the movements of individuals from a higher to lower concentration region. Self-diffusion coefficients are denoted by $d_1$ and $d_2$, respectively [8].

Non-zero initial conditions

$$N(x, y, 0) > 0; P(x, y, 0) > 0 \tag{3}$$

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

$$\frac{\partial N}{\partial n} = \frac{\partial P}{\partial n} = 0; (x, y) \in \partial\Omega, \tag{4}$$

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.

The first step in analyzing the model is to determine the equilibria (stationary states) of the non-spatial model obtained by setting space derivatives equal to zero, i.e.,

$$\begin{gathered} r\left(1 - \frac{N}{K}\right) N - \frac{\beta N}{B + N + wP} P = 0, \\ \frac{\varepsilon \beta N}{B + N + wP} P - \eta P = 0. \end{gathered} \tag{5}$$

In fact, physically, an equilibrium represents a situation without "life". It may mean no motion of a pendulum, no reaction in a reactor, no nerve activity, no flutter of an airfoil, no laser operation, or no circadian rhythms of biological clocks. And at each equilibrium point, the movement of the population dynamics vanishes.

In the absence of diffusion, the model has three equilibria in the positive quadrant [8]:

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 non-trivial stationary state $(N^*, P^*)$ (coexistence of preys and predators), where

$$\begin{aligned} N^* &= \frac{1}{2rw\varepsilon} K (rw\varepsilon - \varepsilon\beta + \eta) \\ &+ \frac{1}{2rw\varepsilon} \sqrt{K^2 (rw\varepsilon - \varepsilon\beta + \eta)^2 + 4rKw\varepsilon\eta B}, \\ P^* &= \frac{(\beta\varepsilon - \eta)}{w\eta} N^* - \frac{B}{w}. \end{aligned} \tag{6}$$

The numerical model of predator-prey system is based on standard five-point approximation for 2D Laplacian with the zero-flux boundary conditions. The concentrations $\left(N_{ij}^{n+1}, P_{ij}^{n+1}\right)$ at the moment $(n+1)\tau$ at mesh position $(x_i, y_j)$ are calculated as [8]:

$$\begin{aligned} N_{ij}^{n+1} &= N_{ij}^n + \tau d_1 \Delta_h N_{ij}^n + \tau f\left(N_{ij}^n, P_{ij}^n\right), \\ P_{ij}^{n+1} &= P_{ij}^n + \tau d_2 \Delta_h P_{ij}^n + \tau g\left(N_{ij}^n, P_{ij}^n\right), \end{aligned} \tag{7}$$

where the Laplacian is

$$\Delta_h N_{ij}^n = \frac{N_{i+1,j}^n + N_{i-1,j}^n + N_{i,j+1}^n + N_{i,j-1}^n - 4N_{i,j}^n}{h^2}. \tag{8}$$

Initially, the entire system is placed in the stationary state $(N^*, P^*)$ with a random perturbation. The system evolves either into 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: stripe-like patterns, regular spotted pattern, the mixture of spotted and stripe-like patterns or the spiral wave patterns [8].

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

We use Beddington-DeAngelis-type predator-prey model with self-diffusion with the following parameter set: $d_1 = 0.01$, $d_2 = 1$, $r = 0.5$, $\varepsilon = 1$, $\beta = 0.6$, $K = 2.6$, $\eta = 0.25$, $\omega = 0.4$, $B = 0.3154$. All our numerical simulations employ the Neumann (zero-flux) boundary conditions with a system size of $200 \times 200$ space units ($L_x = L_y = 50$). The system in Eq. (1) is solved numerically in two-dimensional space using a finite difference approximation for the spatial derivatives and an explicit Euler method for the time integration (Eq. (7)) with a time step $\tau = 0.01$ and space step $h = 0.25$. The scale of the space and time are average to the Euler method.

The dynamics of the time evolution of preys $N$ is demonstrated in Fig. 1. Fig. 1(a) presents the equilibrium point $(N^* = 0.43058; P^* = 0.718555)$ with small random perturbations.

We use the logistic map

$$x_{i+1} = \mu x_i (1 - x_i) \tag{9}$$

with $\mu = 4$ for the computation of a set of $200 \times 200$ pseudo-random numbers distributed in the interval $[0; 1]$. The dynamics of the logistic map depends on the value of parameter $\mu$. When $\mu = 4$, system in Eq. (9) demonstrates chaotical behavior and therefore is appropriate for the generation of random numbers.

The obtained random set distributed in the interval $[0; 1]$ is linearly transformed into an $\varepsilon$-length interval with zero mean and is added to the initial concentration of preys:

$$[N]|_{t=0} = N^* \cdot [1] + \left[\widetilde{N}\right]; [P]|_{t=0} = P^* \cdot [1], \tag{10}$$

where $[1]$ is a $200 \times 200$ matrix of ones; $\left[\widetilde{N}\right]$ is a $200 \times 200$ matrix of pseudo-random numbers distributed uniformly in the interval $[-\varepsilon/2; \varepsilon/2]$. It is clear that the parameter $\varepsilon$ 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.

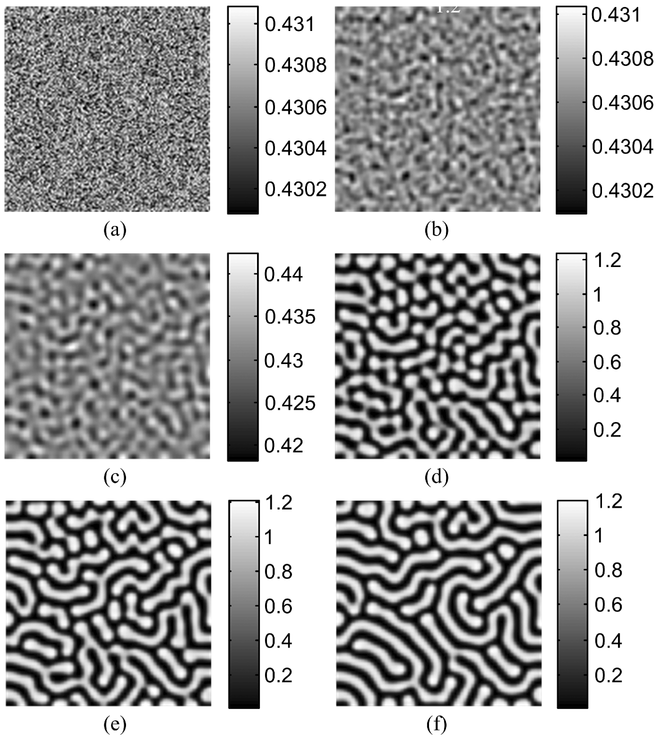

Fig. 1. Dynamics of the time evolution of preys: (a) – the initial distribution ($\varepsilon = 10^{-3}$); (b) – after 2500 iterations; (c) – after 10000 iterations; (d) – after 25000 iterations; (e) – after 50000 iterations; (f) – after 200000 iterations.

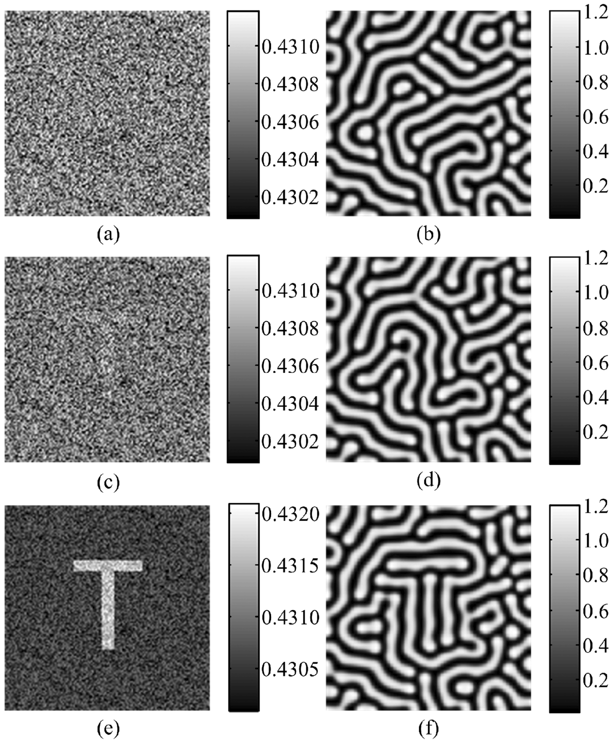

Fig. 2. Time evolution of preys: (a) – the initial density of preys ($\varepsilon = 10^{-3}$; $\delta = 0$); (b) – the pattern of preys after 200000 iterations. (c) and (e) represent initial densities of preys distorted by the T-shaped mask at $\delta/\varepsilon = 0.1$ and $\delta/\varepsilon = 1$ respectively (the same matrix $\left[\widetilde{N}\right]$ is used in all experiments). (d) and (f) illustrate patterns of preys after 200000 iterations.

Fig. 1(b), Fig. 1(c), Fig. 1(d) and Fig. 1(e) show the evolution of the spatial pattern of preys after 2500, 10000, 25000 and 50000 iterations. Time-independent self-organizing pattern of stripes and spots is obtained after 200000 iterations (Fig. 1(f)). It is important to note that the pattern shown in Fig. 1(f) is sensitive to initial conditions. Fig. 2(a) shows the initial distribution of preys and Fig. 2(b) represents the pattern after 200000 iterations (all parameters of the system are kept the same). Different initial perturbations in Eq. (10) (a different set of pseudo-random numbers) evolve into a pattern of the same type as shown in Fig. 1(f) but with a different writing.

### *A. The generation of target patterns*

The evolution of self-organizing patterns is sensitive to initial perturbations. This fact allows construction and manipulation of target patterns by small modifications in the initial distribution of preys. Fig. 1(f) and Fig. 2(b) illustrates that two different realizations of initial concentrations of preys result into apparently similar but locally different patterns of stripes.

Let us assume that the matrix of random perturbations $\left[\widetilde{N}\right]$ is modified by adding a positive constant $\delta$ 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:

$$[N]|_{t=0} = N^* \cdot [1] + \left[\widetilde{N}\right] + \delta \cdot [M], \tag{11}$$

where $\delta$ 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 $\delta$ and zeroes where the random density of preys is kept unchanged.

It is clear that different levels of $\delta$ would lead to the different patterns when the system evolves in time.

Let us assume that the initial random density of preys (shown in Fig. 2(a)) is changed by adding a T-shaped mask. Numerical values of pixels in the zone occupied by the letter T are incremented by $\delta$; all other pixels remain unchanged. Fig. 2(c) and 2(e) represent modifications of the initial distribution of preys for different values of $\delta$. It appears that the striped-spotted pattern of preys mimics the shape of the mask after 200000 iterations if only $\delta$ is sufficiently high. It can be noted that a larger ratio $\delta/\varepsilon$ corresponds to a clearer target image in final patterns (Fig. 2(f)). Unfortunately, the ratio $\delta/\varepsilon = 0.1$ (Fig. 2(c)) does not yield an interpretable pattern (Fig. 2(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. 2(c).

Therefore, such an approach can not be considered as a safe technique for encoding secret information.

### *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 consid-

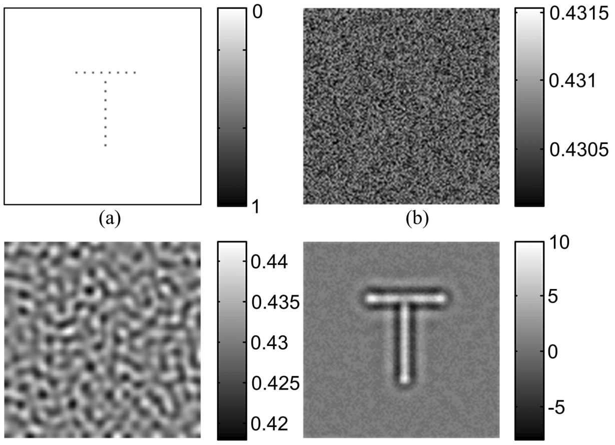

Fig. 3. A steganographic communication scheme based on the difference between evolving patterns. (a) – the dot-skeleton representation of the secret image; (b) – the perturbed initial distribution of preys; $\delta/\varepsilon = 0.3$; (the initial distribution of preys is shown in Fig. 1(a)); (c) – time evolution of (b) after 10000 iterations; (d) – the difference between (c) and Fig. 1(c).

ered as a safe encoding of secret visual information – the target pattern becomes interpretable only when the initial distribution of preys leaks 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.

At first we construct the initial random distribution of preys (Eq. (10)) and compute the density of preys after the system evolves $m$ iterations in time (Fig. 1(a) and Fig. 1(c)). In the next step the initial random distribution of preys is perturbed. We use Eq. (11) for the perturbation, but the mask $[M]$ now holds not a target pattern but skeleton dots of the secret image instead (Fig. 3(a)). It can be noted that the matrix $\left[\tilde{N}\right]$ must be kept the same in both computational experiments and that $\delta$ is low enough to prevent statistical identification of the perturbation (we use $\delta/\varepsilon = 0.3$ in Fig. 3(b)). Now, the density of preys is computed after the system evolves $m$ iterations in time (Fig. 3(c)). In fact, differences between Fig. 1(c) and Fig. 3(c) are hardly seen. Anyway, we compute the difference between these two patterns; the resulting image is shown in Fig. 3(d). It can be noted that the colorbar in Fig. 3(d) shows the difference in pixel levels (grayscale levels are measured in the interval $[0; 255]$), while colorbars in Fig. 3(b) and 3(c) show actual concentration of preys.

The secure communication system based on the formation of self-organizing patterns can be described by the schematic diagram in Fig. (4).

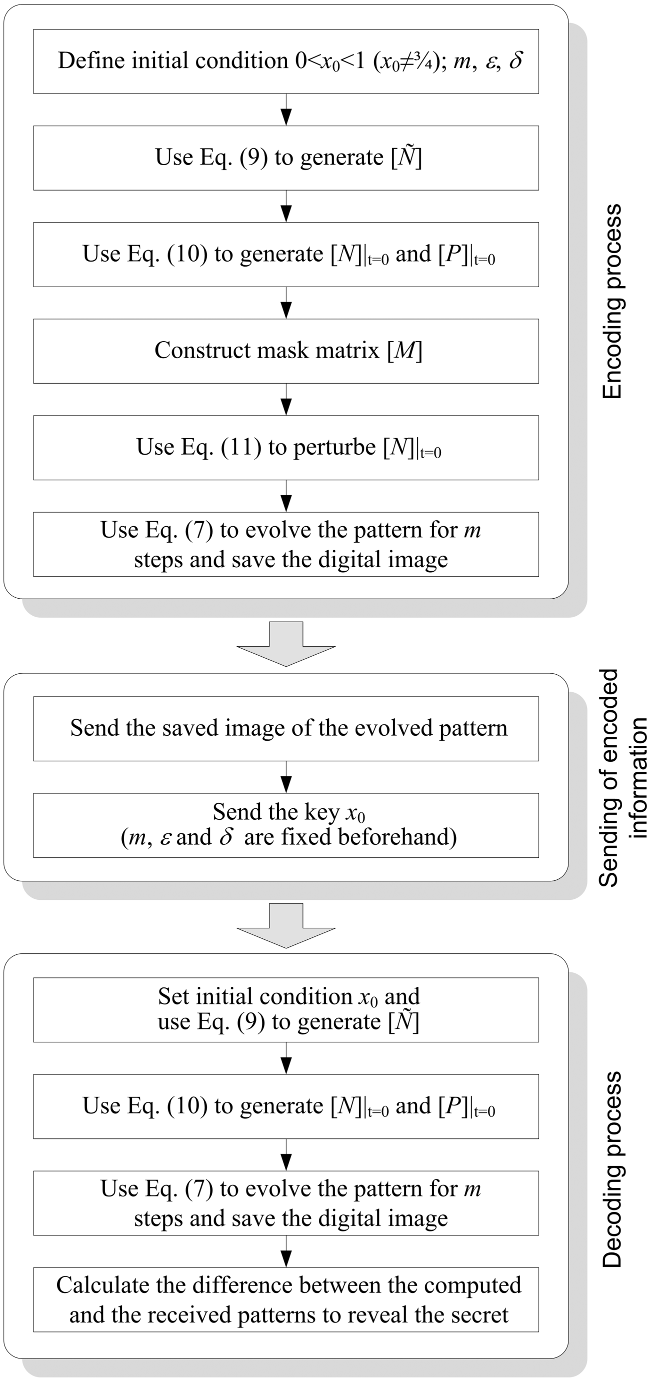
Define initial condition 0<$x_0$<1 ($x_0$≠¾); $m$, $\varepsilon$, $\delta$
Use Eq. (9) to generate [$\tilde{N}$]
Use Eq. (10) to generate $[N]|_{t=0}$ and $[P]|_{t=0}$
Construct mask matrix [$M$]
Use Eq. (11) to perturbe $[N]|_{t=0}$
Use Eq. (7) to evolve the pattern for $m$ steps and save the digital image
Encoding process
Send the saved image of the evolved pattern
Send the key $x_0$ ($m$, $\varepsilon$ and $\delta$ are fixed beforehand)
Sending of encoded information
Set initial condition $x_0$ and use Eq. (9) to generate [$\tilde{N}$]
Use Eq. (10) to generate $[N]|_{t=0}$ and $[P]|_{t=0}$
Use Eq. (7) to evolve the pattern for $m$ steps and save the digital image
Calculate the difference between the computed and the received patterns to reveal the secret
Decoding process

Fig. 4. Schematic diagram of the secure communication system based on the formation of self-organizing patterns.

The functionality of the proposed technique is demonstrated using a computational example illustrated in Fig. 5. The secret image is shown in Fig. 5(a); its dot-skeleton representation – in Fig. 5(b) (the distance between dots in the direction of the $x-$ and $y-$ axis is 7 pixels). The encrypted image is shown in Fig. 5(c); the evolved pattern from the encrypted image (after 10000 iterations) is shown in Fig. 5(d). The evolved pattern from the random perturbation (without the embedded dot-skeleton representation of the secret image) is shown in Fig. 5(e). The difference between Fig. 5(d) and Fig. 5(e) is shown in Fig. 5(f).

A naked eye can not see any differences between Fig. 5(d) and Fig. 5(e). But it is important to note that the actual difference between Fig. 5(d) and Fig. 5(e) is a smooth image; the secret information is not hidden at some isolated pixels. Steganalysis procedures [15] would not be able to detect the

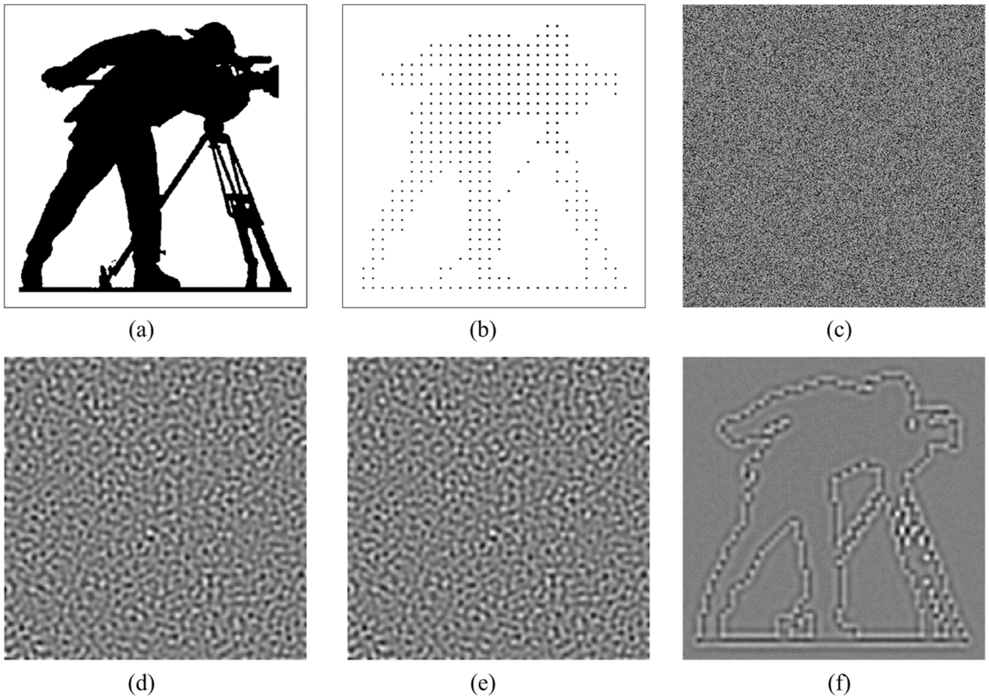

Fig. 5. The illustration of steganographic visual communication system based on self-organizing patterns: (a) – the secret image; (b) – the dot-skeleton representation of the secret image; (c) – the random initial distribution of preys with the embedded dot-skeleton representation of the secret image; (d) – time evolution of (c) after 10000 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 (d) and (e) reveals the secret image.

fact that some secret information is being transmitted by means of Fig. 5(d).

## IV. Advantages 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 [16], algorithms using the transform domain such as F5 [17] and algorithms taking an adaptive approach combined with one of the former two methods, e.g., ABCDE (A block-based complexity data embedding) [18]. 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. 3 bits in each pixel can be stored by modifying the LSBs of 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 [19], [20]. The LSB modification concept can be used to hide data in an image [20], [21]. A random LSB insertion method is developed in [22] where the secret data are spread out among the cover image in a seemingly random diffused manner. An LSB insertion steganographic method coupled with high security digital layers is presented in [23]. A heuristic approach to hide data using LSB steganography technique is proposed in [24].

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 [13]. We transmit a smooth pattern which has evolved from perturbed initial conditions. It would be impossible to trace a perturbed pixel in the digital image of the evolved pattern.

## V. Concluding remarks

A new steganographic communication scheme based on evolving patterns is proposed in this paper. We use the perturbed pattern of preys to hide the skeleton of the secret image.

We have exploited the well-known Beddington-DeAngelis-type predator-prey model with self-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, which 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.

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.

## References

[1] L. Saunoriene and M. Ragulskis, "A secure steganographic communication algorithm based on self-organizing patterns," *Phys. Rev. E*, vol. 84, p. 056213, 2011.

[2] J. E. Pearson, "Complex patterns in a simple system," *Science*, vol. 261(5118), pp. 189–192, 1993.

[3] M. Seul and D. Andelman, "Domain shapes and patterns:the phenomenology of modulated phases," *Science*, vol. 267(5197), pp. 476–483, 1995.

[4] O. Kuksenok, V. V. Yashin, and A. C. Balazs, "Spatial confinement controls self-oscillations in polymer gels undergoing the belousov-zhabotinsky reaction," *Phys. Rev. E*, vol. 80, p. 056208, 2009.

[5] A. Yochelis and M. Sheintuch, "Principal bifurcations and symmetries in the emergence of reaction-diffusion-advection patterns on finite domains," *Phys. Rev. E*, vol. 80, p. 056201, 2009.

[6] C. M. Topaz and A. J. Catllá, "Forced patterns near a turing-hopf bifurcation," *Phys. Rev. E*, vol. 81, p. 026213, 2010.

[7] Y. Suzuki, T. Takayama, I. N. Motoike, and T. Asai, "Striped and spotted pattern generation on reaction-diffusion cellular automata: Theory and lsi implementation," *Int. J. Unconv. Comput.*, vol. 3, pp. 1–13, 2007.

[8] W. Wang, Y. Lin, L. Zhang, F. Rao, and Y. Tan, "Complex patterns in a predator-prey model with self and cross-diffusion," *Commun. Nonlinear Sci. Numer. Simulat.*, vol. 16, pp. 2006–2015, 2011.

[9] W. Wang, L. Zhang, H. Wang, and Z. Li, "Pattern formation of a predator-prey system with ivlev-type functional response," *Ecol. Model.*, vol. 221(2), pp. 131–140, 2010.

[10] M. R. Garvie and C. Trenchea, "Spatiotemporal dynamics of two generic predator-prey models," *J. Biol. Dynamics*, vol. 4(6), pp. 559 – 570, November 2010.

[11] B. Dubey, N. Kumari, and R. K. Upadhyay, "Spatiotemporal pattern formation in a diffusive predator-prey system: an analytical approach," *J. Appl. Math. Comput.*, vol. 31, pp. 413–432, 2009.

[12] V. V. Yaschenko, *Cryptography: An Introduction*. Providence, RI: American Mathematical Society, 2002.

[13] N. Johnson, Z. Duric, and S. Jajodia, *Information hiding: steganography and watermarking: attacks and countermeasures*. Netherlands: Springer, 2001.

[14] F. A. P. Petitcolas and S. Katzenbeisser, *Information Hiding Techniques for Steganography and Digital Watermarking*. Boston: Artech House Publishers, 2000.

[15] H. Wang and S. Wang, "Cyberwarfare: Steganography vs steganalysis," *Communications of the ACM*, vol. 47, p. 76, 2004.

[16] "Online software [s-tools]," accessed 15-August-2011, ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip.

[17] "Online software [f5]," accessed 15-August-2011, http://wwwrn.inf.tu-dresden.de/∼westfeld/f5.html.

[18] H. Hioki, in *Proceedings of Pacific Rim Workshop on Digital Steganography*, July 2002, p. 30.

[19] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, p. 26, 1998.

[20] S. Bandyopadhyay, D. Bhattacharyya, P. Das, S. Mukherjee, and D. Ganguly, "A tutorial review on steganography," in *IC3*, August 2008, p. 106.

[21] K. M. Singh, S. B. Singh, and L. S. S. Singh, "Hiding encrypted message in the features of images," *IJCSNS*, vol. 7, p. 302, 2007.

[22] M. Sutaone and M. Khandare, "Image based steganography using lsb insertion technique," in *IEEE WMMN*, January 2008, p. 146.

[23] N. N. EL-Emam, "Hiding a large amount of data with high security using steganography algorithm," *J. Comp. Sci.*, vol. 3, p. 223, 2007.

[24] S. K. Bandyopadhyay, D. Bhattacharyya, P. Das, S. Mukherjee, and D. Ganguly, "A secure scheme for image transformation," in *IEEE SNPD*, August 2008, p. 490.