Physica A 443 (2016) 91–97

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Competitively coupled maps for hiding secret visual information

M. Vaidelys, P. Ziaukas, M. Ragulskis *

Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50, Kaunas LT-51368, Lithuania

HIGHLIGHTS

- Competitively maps are used for hiding digital images.
- Non-diffusive coupling results into relatively short-transients.
- Secret image is embedded into initial state far below the noise level.

ARTICLE INFO

Article history:
Received 21 April 2015
Received in revised form 28 June 2015
Available online 25 September 2015

Keywords:
Self-organizing pattern
Competitive coupling
Image hiding

ABSTRACT

A novel digital image hiding scheme based on competitively coupled maps is presented in this paper. Self-organizing patterns produced by an array of non-diffusively coupled nonlinear maps are exploited to conceal the secret. The secret image is represented in the form of a dot-skeleton representation and is embedded into a spatially homogeneous initial state far below the noise level. Self-organizing patterns leak the secret image at a predefined set of system parameters. Computational experiments are used to demonstrate the effectiveness and the security of the proposed image hiding scheme.

1. Introduction

The understanding of evolution of spatial patterns in simple systems remains an active research area. One of the classical models of irregular spatiotemporal patterns emerging dynamically from a spatially homogeneous initial state comprises a simple reaction–diffusion system with finite amplitude perturbations [1]. Small perturbations of initial states play a central role in the initiation of pattern formation process, whereas spontaneous self-organization yields patterns in a purposeful manner without external stimulation [2]. The diffusion of the competing species (under suitable conditions) can drive symmetry breaking in the initial homogeneous configuration [3]. Typically, situation-dependent necessary conditions must be enforced in order to ensure the emergence of spatial patterns from homogeneous initial conditions [4].

It is well known that spatial self-organizing patterns can be effectively used for hiding secret visual images. A digital fingerprint image is used as the initial condition for the evolution of a pattern in a model of reaction–diffusion cellular automata [5]. 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 Ref. [6]. Self-organizing patterns induced by complex interactions between competing individuals and described by evolutionary spatial 2×2 games are exploited for hiding and transmitting secret visual information in Ref. [7]. It is natural to expect that other nonlinear models of self-organizing systems could be also applicable for hiding secret visual images.

* Corresponding author. Tel.: +370 698 22456.
E-mail addresses: martynas.vaidelys@ktu.lt (M. Vaidelys), pranas.ziaukas@ktu.edu (P. Ziaukas), minvydas.ragulskis@ktu.lt (M. Ragulskis).

http://dx.doi.org/10.1016/j.physa.2015.09.044
0378-4371/

The main objective of this paper is to seek such a nonlinear self-organizing system which would enable to construct a relatively simple but computationally effective visual communication algorithm. At least 10 000 time forward iterations are required for the reaction–diffusion model in Ref. [6] to exhibit an interpretable pattern. The inversion of a single pixel in the dichotomous random image of initial conditions does not result into any changes in the difference image in the communication algorithm proposed in Ref. [7]. This fact is based on the property of evolutionary spatial 2×2 games where the strategy of a single individual does not determine the resulting strategy of the whole population.

An effective application of a communication algorithm based on self-organizing patterns needs to satisfy several important requirements. First of all, this algorithm should be steganographically secure. Image steganography is the science of concealing secret images within other digital cover images [8]. The advantage of steganography, over cryptography alone, is that steganography can be said to protect both messages and communicating parties, whereas cryptography protects only the contents of a message [9]. Secondly, the secret visual information should be encoded in the random image of the initial conditions by using slight modifications of only several individual pixels; all modifications should be lower than the noise level of the initial conditions. Finally, the communication algorithm should be computationally effective—the number of time forward steps used for the development of self-organizing patterns should be small. Clearly, all existing communication algorithms based on self-organizing patterns do not satisfy all three requirements. The algorithm in Ref. [5] is not steganographically secure because distinct visual patterns are not hidden in cover images. Visual patterns can draw attention from eavesdroppers and thus are prone to being thoroughly analyzed and uncovered (in other words the principles of steganography fail to hold). The technique in Ref. [6] requires a large number of time forward steps and is not computationally effective; the method in Ref. [7] requires the modification of large blocks of pixels in the random image of initial conditions.

This paper is organized as follows. The model of the system is presented in Section 2; the communication scheme is presented in Section 3; the sensitivity of the scheme to the perturbation of the systems parameters is discussed in Section 4; concluding remarks are given in the final section.

2. The model of the system

Let us consider a one-dimensional unimodal mapping in the form $f(x) = x \cdot F(x)$ where $F : \mathbb{R} \to \mathbb{R}$ is a smooth mapping. We will use $F(x) = \lambda(1 + x^b)$ named after Maynard Smith [10] where parameters λ and b are positive constants.

A two-dimensional generalization of this mapping with the introduction of the competitive aspect to the model, gives the time evolution of a particular state $x(t)$ at time t on a rectangular domain $[1; L_x] \times [1; L_y]$:

$$x_{i,j}(t+1) = x_{i,j}(t) \cdot F[x_{i,j}(t) + \alpha \cdot \Sigma_{i,j}(t)] \tag{1}$$

where

$$\Sigma_{i,j}(t) = \sum_{\substack{p,q\in\{-1,0,1\} \\ (p,q)\neq(0,0)}} x_{k,l}(t), \qquad k = \mathrm{mod}(i+p-1, L_x) + 1;\ l = \mathrm{mod}\left(j+q-1, L_y\right) + 1 \tag{2}$$

is the sum of adjacent elements in the 8-element Moore neighborhood of the element $x_{i,j}(t)$; α is a nonnegative parameter that represents the strength of the competitive interaction between neighboring elements. Note that the local site dynamics are coupled through a competitive, rather than diffusive, interaction. 2D periodic boundary conditions are assumed; L_x and L_y define the number of elements in the rectangular domain. Note that every element $x_{i,j}$ represents a single pixel of a digital image.

Competitively coupled maps are based on interactions between discrete neighboring nodes. These interactions are usually interpreted as the competition from the physical (or biological) point of view. In terms of steganography, it is always important to take into account algorithmic aspects of the evolutionary model—such as feasibility, computational efficiency and complexity, memory and time requirements. A large variety of different evolutionary models exhibiting interesting behavioral aspects does exist. However, competitively coupled maps are relatively simple yet robust and computationally effective models capable of producing stationary patterns from homogeneous initial configurations—and therefore are well suited for the considered steganographic application. Moreover, competitively coupled maps presented in Ref. [10] do produce complex spatial patterns even when the dynamics at each node is trivial (the local dynamics of an isolated node does exhibit a stable fixed point). This is in stark contrast to conventional diffusively coupled map lattices where trivial dynamics of a node can only result in a spatially homogeneous state [11–13].

2.1. Initial conditions

Initial states of all elements are set as randomly distributed numbers over the interval $[0, 1]$. The chaotic logistic map [14] could be used for the efficient generation of these states—communicating parties can share only the initial condition of the logistic map instead of sharing initial states of all elements in the domain. Iterated values of the logistic map

$$a_{i+1} = 4a_i(1 - a_i) \tag{3}$$

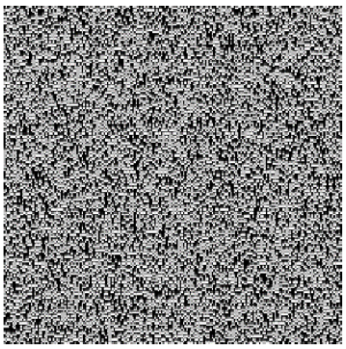

Fig. 1. Pseudorandom initial conditions generated sequentially by the logistic map; the initial value $a_0 = 0.05$; dimensions $L_x = L_y = 200$.

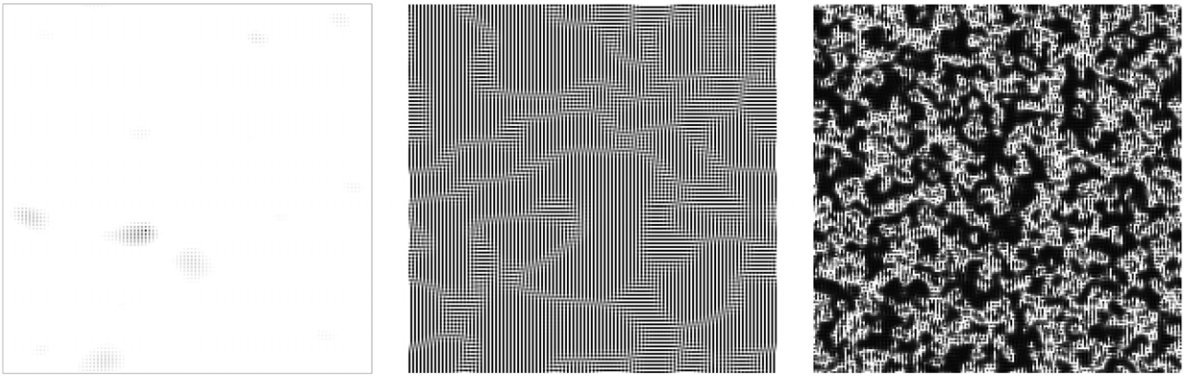

Fig. 2. Patterns produced by the Maynard Smith map depend on the system's parameters. The set of parameters $\lambda = 5, \alpha = 0.25, b = 1$ does not produce an interpretable pattern even after 300 iterations (part a). $\lambda = 4, \alpha = 0.26, b = 2$ produce an interpretable pattern after 300 iterations (part b). $\lambda = 7, \alpha = 0.3, b = 4$ also result into a developed pattern after only 6 iterations (part c). All three patterns are generated from the same initial conditions in Fig. 1.

are used to fill the consecutive elements of 200×200 domain (the initial digital image is illustrated in Fig. 1). And though the logistic map is used in many image encryption algorithms [15,16], it has some drawbacks as a relatively small key space and non-uniform distribution of sequences over the interval [0, 1] (these defects may be utilized by the attackers). The intertwined logistic map [17] could be used in order to overcome all the drawbacks of the logistic map. Nevertheless, we continue computational experiments with the standard logistic map.

2.2. Self-organizing patterns

It is clear that the parameters of the Maynard Smith function (λ and b), the strength of the competitive interaction between neighboring elements α and the number of iterations n have a strong effect on the formation of self-organizing patterns given a spatially homogeneous initial state. Different combinations of these parameter values result into the formation of different patterns (or even the absence of interpretable patterns at all)—some typical situations are illustrated in Fig. 2. The set of parameters $\lambda = 5, \alpha = 0.25, b = 1$ does not produce an interpretable pattern even after 300 iterations from the initial conditions shown in Fig. 1 (Fig. 2(a)). Parameters $\lambda = 4, \alpha = 0.26, b = 2$ yield an interpretable pattern after 300 iterations (Fig. 2(b)) from the same initial conditions. Finally, $\lambda = 7, \alpha = 0.3$ and $b = 4$ also result into a developed pattern but after only 6 iterations (Fig. 2(c)) from the same initial conditions. The size of all digital images in Fig. 2 is $L_x = L_y = 200$; periodic boundary conditions are set along the borders of the image.

3. A communication scheme based on self-organizing patterns

Self-organizing patterns (SOP) can be efficiently exploited as cover images for the transmission of secret visual information. The communication scenario between the Sender and the Receiver can be described by the scheme below (see Steps 1–6).

Sender and Receiver can use an asymmetric (arbitrary) protocol in order to determine the initial value a_0, and the number of time-forward iterations n for SOP generation (parameters of SOP λ, α, b, L_x, L_y must be predetermined beforehand).

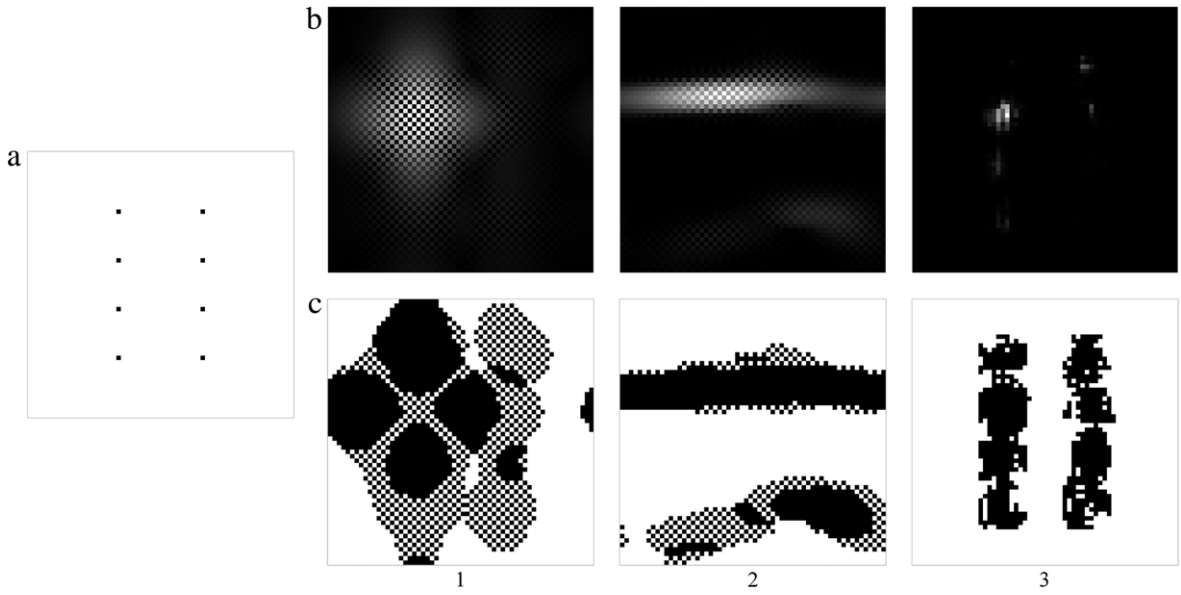

Fig. 3. The difference image between the patterns produced by random initial conditions and modified initial conditions by the dot-skeleton representation as shown in part (a). Column 1 represents the set of parameters $\lambda = 5$, $\alpha = 0.25$, $b = 1$; column 2—the set of parameters $\lambda = 4$, $\alpha = 0.26$, $b = 2$; column 3—the set pf parameters $\lambda = 7$, $\alpha = 0.3$, $b = 4$. Difference images are presented in row (b); difference images with enhanced contract in row (c). Parameter sets in columns (1) and (2) do fail to recreate the hidden information, while the parameter set in column (3) produces a satisfactory result.

1. Sender generates the pseudo-random matrix of initial conditions (as introduced in Section 2.1) by using the Logistic map and the value a_0; the size of the matrix is $L_x \times L_y$.
2. Sender modifies the pseudo-random matrix of initial conditions by adding or subtracting a small number δ to/from some pixels. Usually, δ is much lower than the range (the difference between the highest and the lowest values) of the initial conditions.
3. Sender executes the SOP n forward iteration algorithm (as introduced in Section 2.2) starting from the modified initial conditions and sends the SOP image to the Receiver.
4. Receiver generates the pseudo-random matrix of initial conditions by using the Logistic map and the value a_0; the size of the matrix is $L_x \times L_y$ (this is an identical image to the one generated by the Sender in Step 1).
5. Receiver executes the SOP n forward iteration algorithm starting from the non-modified initial conditions.
6. Finally, the difference between the SOP image produced by the non-modified and modified initial conditions reveals the secret.

It is worth noting that instead of the whole dichotomic silhouette of the secret image one may use skeleton dots corresponding to the contour instead (the dot-skeleton representation of the secret image).

It is clear that not all values used as SOP parameters (λ, α, b) would be applicable for such a communication scheme (even if the values of parameters do ensure the evolution of a well-developed SOP). Let us assume that a dot-skeleton representation of the secret image is a regular array dots (Fig. 3(a)). We set $\delta = 0.01$ and modify the image of pseudorandom initial conditions in Fig. 1 by randomly adding or subtracting 0.01 to/from the grayscale level of corresponding pixels. Note that the values of pixels generated by the chaotic Logistic map are distributed in the interval [0, 1]—thus all perturbations we make are much weaker than the noise level of the initial conditions.

It is natural to expect that the first parameter set used in Fig. 2 would not produce any interpretable pattern in the difference image—the perturbation in the initial conditions causes some uninterpretable fluctuations in the difference image (Fig. 3(b), column 1). The contrast of the difference image can be sharpened using digital morphological operations (Fig. 3(c), column 1)—but the difference image is still uninterpretable.

But, surprisingly, the second parameter set used in Fig. 2 does not produce any meaningful information either (Fig. 3(b) and (c), column 2). However, the third set of parameters does produce an interpretable pattern in the difference image (Fig. 3(b) and (c), column 3).

Fig. 4 illustrates the formation of two parallel lines in the difference image from the dot-skeleton representation of these lines in the random image of initial conditions. It is clear that different distances between dot-skeleton points may not result into the formation of continuous lines in the difference image. Thus, the optimal density of dot-skeleton points for the formation of continuous line-type objects in the difference image is 10 pixels; note that the width of the resulting lines is about 13 pixels (Fig. 4 part (a)).

Finally, the communication scheme based on SOP generated by competitively coupled maps can be illustrated by the following flow chart diagram in Fig. 5. The original secret image is shown in part a; the dot-skeleton representation of the

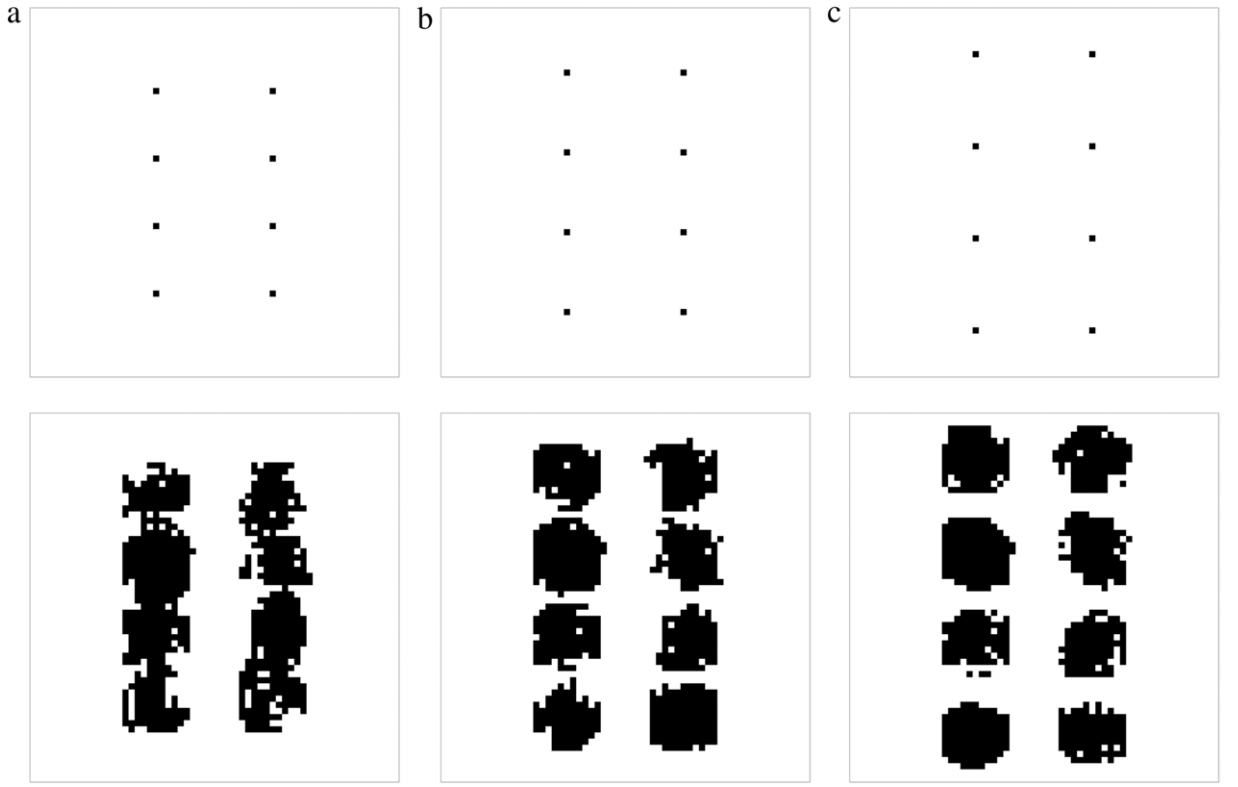

Fig. 4. The optimal density of dot-skeleton points in case of parameters $n = 6$, $L_x = L_y = 50$, $\lambda = 8$, $\alpha = 0.3$, $b = 4$. Figures in the upper row show the dot-skeletons, figures in the lower row illustrate the highlighted difference images. Distances between skeleton dots in cases (a), (b) and (c) are 10, 12 and 14 respectively.

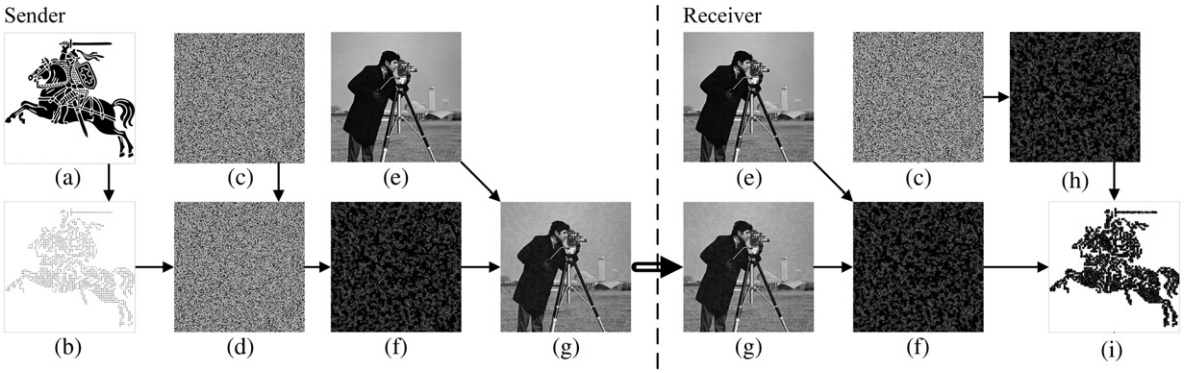

Fig. 5. Flow chart diagram of the communication algorithm. Original image (a); dot-skeleton representation (b); initial conditions (c); perturbed initial conditions (d); cover image (e); perturbed self-organizing pattern (f); perturbed cover image (g); self-organizing pattern (h); difference image (i).

secret image is shown in part b. The sender retrieves the parameter a_0 and generates the random image of initial conditions by using the Logistic map (part c). The dot-skeleton representation of the secret image is embedded into the random image of initial conditions by randomly adding or subtracting 0.01 to/from the corresponding pixels of the random image (part d). Note that all deformations of the image of initial conditions are far below the noise level.

Next, the sender executes the pattern formation algorithm and produces the SOP image (part f) from the modified initial conditions (part d). In order to conceal the transmission of a suspicious image of SOP, the sender uses a standard cover image (part e) and a standard least significant bit based stenographic algorithm for hiding the SOP image (part f) in the cover image. The resulting image (part g) is transmitted to the receiver.

The receiver uses the same cover image (part e) and the received image (part g) to reproduce the SOP image (part f). Note that the SOP image (part f) has been produced from the initial conditions with the embedded dot skeleton representation of the secret image.

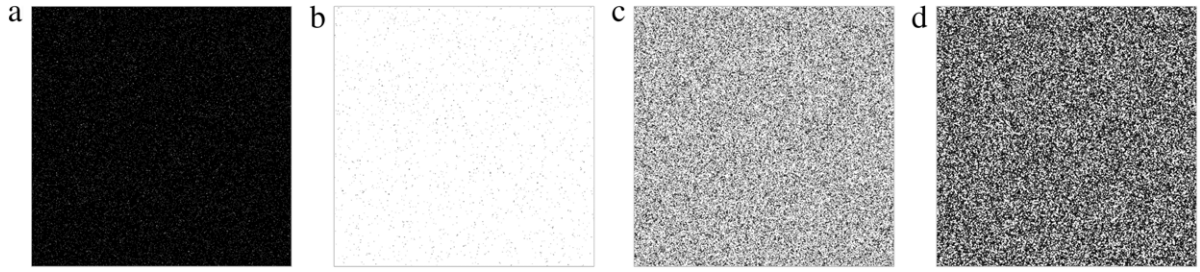

Fig. 6. Initial parameters used by the Sender are: $a_0 = 0.05$, $\lambda = 7$, $\alpha = 0.3$, $b = 4$. The perturbation of one parameter by the Receiver results into an uninterpretable difference image (a single perturbation of one parameter is used in every part respectively): (a) $a_0 = 0.0501$; (b) $\lambda = 7.01$; (c) $\alpha = 0.301$; (d) $b = 4.01$.

Then, the receiver retrieves the parameter a_0 and generates the random image of the initial conditions by using the Logistic map (part c). The receiver uses the identical pattern formation algorithm as used by the sender and produces his copy of the SOP image (part h). The difference image between two SOP images reproduces the secret (part i).

4. Sensitivity of the communication scheme to the perturbation of parameters

As mentioned previously, the presented communication scheme does function at preset values of system's parameters. Slight changes of these parameters (when the Sender and the Receiver use different parameters) may compromise the communication system.

Fig. 6 illustrates the sensitivity of the communication system to slight perturbations; all illustrations represent difference images in the enhanced contrast mode (similarly as used in Figs. 3–5). Initially, we perturb the random initial conditions. The Sender uses all system's parameters as preset in the computational experiment illustrated in Fig. 5 ($a_0 = 0.05$, $\lambda = 7$, $\alpha = 0.3$, $b = 4$)—but the Receiver uses $a_0 = 0.0501$ instead of $a_0 = 0.05$. The chaotic Logistic map is sensitive to small perturbations—thus it is natural to expect that the evolving patterns from different initial conditions would result into a completely different SOP image which is not applicable for the reconstruction of the embedded secret. As expected, the resulting difference image (Fig. 6(a)) is completely uninterpretable.

The next computational experiment simulates the attack of the parameter λ. The receiver mistreats the parameter λ by using $\lambda = 7.01$ instead of $\lambda = 7$. The change is crucial enough to make the difference image (Fig. 6(b)) uninterpretable. Analogously, the competitive parameter $\alpha = 0.301$ is used instead of $\alpha = 0.3$. The resulting difference (Fig. 6(c)) is meaningless. Finally $b = 4.01$ is taken instead of $b = 4$ by the receiver. Once again, this results in a failure to obtain a meaningful difference image (Fig. 6(d)).

5. Concluding remarks

Self-organizing patterns can be used to conceal secret images; reaction–diffusion models and evolutionary spatial games had been successfully exploited for these purposes previously. However, reaction–diffusion models do require long transients; evolutionary spatial games are not sensitive to changes in the strategy of a single individual pixel in the initial state of the system.

It appears that competitively and non-diffusively coupled nonlinear maps help to overcome the drawbacks of the mentioned communication schemes. The secret image can be embedded into the spatially homogeneous initial state in a form of a dot-skeleton representation—and far below the noise level of the initial random image. Parameters of the array of competitively coupled maps can be used as private and public keys—thus enabling an efficient and secure communication system based on self-organizing patterns.

Other nonlinear competitively coupled maps could be considered instead of the Maynard Smith map. A possible example could be the Ricker and Hassell maps discussed in Ref. [10], or even some other more complex nonlinear competitively coupled maps. However, the ability of a coupled map to generate self-organizing patterns is not a sufficient condition for the construction of the proposed image hiding scheme. It is important that the difference image between the patterns produced by the non-modified and modified initial conditions would be able to represent the dot-skeleton representation of the secret information. This requirement is far from being trivial and necessitates an appropriate tuning of systems parameters. The employment of other nonlinear competitively coupled maps for image hiding applications remains a definite objective of future research.

Acknowledgment

Financial support from the Lithuanian Science Council under Project No. MIP-078/2015 is acknowledged.

References

[1] M. Seul, D. Andelman, Domain shapes and patterns: The phenomenology of modulated phases, Science 267 (5197) (1995) 476–483. http://dx.doi.org/10.1126/science.267.5197.476. URL http://www.sciencemag.org/content/267/5197/476.abstract.

[2] K.J. Lee, W.D. McCormick, Q. Ouyang, H.L. Swinney, Pattern formation by interacting chemical fronts, Science 261 (5118) (1993) 192–194. http://dx.doi.org/10.1126/science.261.5118.192. URL http://www.sciencemag.org/content/261/5118/192.abstract.

[3] A.M. Turing, The chemical basis of morphogenesis, Philos. Trans. R. Soc. Lond. B Biol. Sci. 237 (641) (1952) 37–72. http://dx.doi.org/10.1098/rstb.1952.0012.

[4] M. Banerjee, S. Abbas, Existence and non-existence of spatial patterns in a ratio-dependent predator–prey model, Ecol. Complex. 21 (0) (2015) 199–214. http://dx.doi.org/10.1016/j.ecocom.2014.05.005. URL http://www.sciencedirect.com/science/article/pii/S1476945X14000580.

[5] Y. Suzuki, T. Takayama, I.N. Motoike, T. Asai, Striped and spotted pattern generation on reaction–diffusion cellular automata—theory and lsi implementation, Int. J. Unconv. Comput. 3 (1) (2007) 1713–1719.

[6] L. Saunoriene, M. Ragulskis, Secure steganographic communication algorithm based on self-organizing patterns, Phys. Rev. E 84 (2011) 056213. URL http://link.aps.org/doi/10.1103/PhysRevE.84.056213.

[7] P. Ziaukas, T. Ragulskis, M. Ragulskis, Communication scheme based on evolutionary spatial games, Physica A 403 (0) (2014) 177–188. http://dx.doi.org/10.1016/j.physa.2014.02.027. URL http://www.sciencedirect.com/science/article/pii/S0378437114001290.

[8] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker (Eds.), The Morgan Kaufmann Series in Multimedia Information and Systems, second ed., Morgan Kaufmann, Burlington, 2008.

[9] S. Katzenbeisser, F.A. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, first ed., Artech House, Inc., Norwood, MA, USA, 2000.

[10] T. Killingback, G. Loftus, B. Sundaram, Competitively coupled maps and spatial pattern formation, Phys. Rev. E 87 (2) (2013) 022902.

[11] I. Waller, R. Kapral, Spatial and temporal structure in systems of coupled nonlinear oscillators, Phys. Rev. A 30 (1984) 2047–2055. http://dx.doi.org/10.1103/PhysRevA.30.2047.

[12] V.A. Jansen, A.L. Lloyd, Local stability analysis of spatially homogeneous solutions of multi-patch systems, J. Math. Biol. 41 (3) (2000) 232–252. URL http://dx.doi.org/10.1007/s002850000048.

[13] P. Rohani, R.M. May, M.P. Hassell, Metapopulation and equilibrium stability: The effects of spatial structure, J. Theoret. Biol. 181 (2) (1996) 97–109. http://dx.doi.org/10.1006/jtbi.1996.0118. URL http://www.sciencedirect.com/science/article/pii/S0022519396901186.

[14] R.M. May, Simple mathematical models with very complicated dynamics, Nature 261 (5560) (1976) 459–467. URL http://dx.doi.org/10.1038/261459a0.

[15] N. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, Image Vis. Comput. 24 (9) (2006) 926–934. http://dx.doi.org/10.1016/j.imavis.2006.02.021. URL http://www.sciencedirect.com/science/article/pii/S026288560600103X.

[16] L. Kocarev, G. Jakimoski, Logistic map as a block encryption algorithm, Phys. Lett. A 289 (4–5) (2001) 199206. URL http://www.sciencedirect.com/science/article/pii/S0375960101006090.

[17] X. Wang, D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, Commun. Nonlinear Sci. Numer. Simul. 18 (11) (2013) 3075–3085. http://dx.doi.org/10.1016/j.cnsns.2013.04.008. URL http://www.sciencedirect.com/science/article/pii/S1007570413001524.