Physica A 403 (2014) 177–188

Contents lists available at ScienceDirect

Physica A

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

Communication scheme based on evolutionary spatial 2 × 2 games

Pranas Ziaukas [a,*], Tautvydas Ragulskis [b], Minvydas Ragulskis [a]

[a] Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-222, Kaunas LT-51368, Lithuania

[b] School of Economics, The University of Edinburgh, 30 Buccleuch Place, Edinburgh EH8 9JT, United Kingdom

HIGHLIGHTS

- A communication scheme based on evolutionary spatial 2 × 2 games is developed.
- Self-organizing patterns are exploited for hiding secret visual information.
- The secure communication scheme can be effectively used for the information exchange.

ARTICLE INFO

Article history:
Received 28 November 2013
Received in revised form 30 January 2014
Available online 22 February 2014

Keywords:
Pattern formation
Steganography
Communication scheme
Spatial game

ABSTRACT

A visual communication scheme based on evolutionary spatial 2 × 2 games is proposed in this paper. Self-organizing patterns induced by complex interactions between competing individuals are exploited for hiding and transmitting secret visual information. Properties of the proposed communication scheme are discussed in details. It is shown that the hiding capacity of the system (the minimum size of the detectable primitives and the minimum distance between two primitives) is sufficient for the effective transmission of digital dichotomous images. Also, it is demonstrated that the proposed communication scheme is resilient to time backwards, plain image attacks and is highly sensitive to perturbations of private and public keys. Several computational experiments are used to demonstrate the effectiveness of the proposed communication scheme.

1. Introduction

Cooperation is the antonym of competition; however the need to compete with others has often induced individuals (genes, cells, organisms, etc.) to organize into a group and cooperate with each other in order to present a stronger competitive force [1–3]. A paradigmatic physical model illustrating the cooperation between competing individuals is the evolutionary spatial 2 × 2 game (ESG).

ESG models are widely discussed in the context of game theory—but they also provide a deep insight into physical properties of self-organizing systems [4–6]. An ESG model where an agent copies a neighbor's strategy based on the highest payoff is proposed in Ref. [7]. Alternatively, an ESG model where an agent copies a neighbor's strategy based on an average payoff of a given strategy is proposed in Ref. [8]. Stochastic inheritance of a neighbor's strategy is studied in Ref. [9]. ESG models where strategies are adopted stochastically based on specific rules (thus behaving like an antiferromagnetic kinetic model) are considered in Ref. [10]. ESG models depicting specific social interactions (in a bottleneck-type environment)

* Corresponding author. Tel.: +370 4437062957744.
E-mail addresses: pranas.ziaukas@ktu.edu (P. Ziaukas), t.ragulskis@sms.ed.ac.uk (T. Ragulskis).
URL: http://www.personalas.ktu.lt/~mragul (M. Ragulskis).

http://dx.doi.org/10.1016/j.physa.2014.02.027
0378-4371/

are studied in Ref. [11]. The importance of cooperation (the so called critical mass) in various ESG models is studied in Ref. [12]. A number of alternative ESG implementations have been proposed: an ESG model with increasing number of neighbors [13]; ESG models with dynamic payoff matrices [14]; ESG models on networks embedded in a space with different kinds of topologies [15]; ESG models where the network structure is not fixed [16].

The main objective of this paper is the development of a new visual communication scheme based on self-organizing patterns produced by ESG. We do adopt a particular ESG model [7], but more sophisticated models could be used for the generation of aforementioned patterns as well.

Self-organizing patterns induced by the Turing instability and produced by Beddington–DeAngelis-type predator–prey model are successfully used in a secure steganographic communication algorithm in Ref. [17]. Thus, another important objective of this paper is to investigate a completely different physical model for the generation of self-organizing patterns and to explore its applicability in the area of visual communication.

This paper is organized as follows: the model of the system is developed in Section 2; the visual communication scheme based on ESG is presented in Section 3; properties of this communication scheme are discussed in Section 4; concluding remarks are given in the final Section 5.

2. The model of the system

2.1. The description of the ESG model

A static 2×2 game is a paradigmatic example in game theory that represents various combinations of individual choices to cooperate or defect given the different 2×2 payoff matrices. A canonical payoff matrix reads:

	P2 cooperates	P2 defects
P1 cooperates	$\boldsymbol{R}, R$	$\boldsymbol{S}, T$
P1 defects	$\boldsymbol{T}, S$	$\boldsymbol{P}, P$

Payoffs for Player 1 (P1) and Player 2 (P2) are shown in bold and normal fonts accordingly. R is the "reward" both players receive if they both cooperate; P is the "punishment" payoff both players receive if they both defect. If P1 defects while P2 cooperates, then P1 receives the "temptation" payoff T while P2 receives the "sucker's" payoff S. Similarly, if P1 cooperates while P2 defects, then P1 receives S while P2 receives T [18].

The most common 2×2 games given different payoff matrices and set of rules are: Prisoner's Dilemma, Hawk–Dove or Chicken, Leader and Stag Hunt games. To be a Prisoner's Dilemma game, the following condition must hold for the payoffs [19]: $T > R > P > S$ and in that case mutual defection is the only strong Nash equilibrium in a finite game [20]. Moreover, the iterated version of Prisoner's Dilemma game is followed by the additional rule $2R > T + S$ in order to prevent alternating cooperation and defection giving a greater reward than mutual cooperation [21,1]. Mutual defection may no longer be a strictly dominant strategy if the number of iterations is random (or at least unknown to the players) [22].

Alternatively, a Stag Hunt game ($R > T > P > S$) emphasizes the idea of mutual cooperation which is likely to bring the greatest rewards for society [23]. However, it requires trust amongst society members (players) and challenges sustained cooperation strategies. For instance, hunting a stag instead of a rabbit requires mutual cooperation of all the hunters and the non-cooperation strategy decreases the chances of stag being hunted.

A Hawk–Dove game requires the following condition for the payoff matrix: $T > R > S > P$ [24]. Now the damage from mutual defection increases because it yields the lowest possible payoff. The most attractive choices for this game become strategies of either mutual cooperation or trying to yield over the other hoping to get the tempting payoff. An unstable equilibrium usually occurs due to this long lasting competition.

A Leader game occurs when the mutual cooperation reward decreases in a Hawk–Dove model resulting into the inequality $T > S > R > P$ [18]. Such payoffs occur in everyday life situations when the strategy of trying to yield over the other is vital and it is much better to win the game alone rather than together. The nature of competition is emphasized and the satisfaction of the other player losing the game is greater than in the case of mutual cooperation or mutual defection. Finally, the game transforms into a Hero game ($S > T > R > P$) when the sucker's payoff is the greatest [18]. A "Heroic" player chooses to play cooperation against a non-cooperative player receiving higher payoff in that case.

Despite the simplicity of such dynamical iterative games, it has been demonstrated that the behavior of such systems is capable of exhibiting an astonishing complexity compared to cellular automata [25,26].

In this paper, we exploit an iterative ESG without memory and without a preselection of a particular type of a game. A player is allowed to interact with its eight immediate neighbors on a regular two-dimensional grid. Each player plays 8 ESG—and his resulting fitness is the sum of individual payoffs.

Let us denote $M(i, j)$ as a player located at ith row and jth column of a rectangular grid with periodic boundaries; $i = 1, 2, \ldots, n$; $j = 1, 2, \ldots, m$; where n and m define the size of the grid with periodic boundaries. The entries of the matrix M are binary digits—1 representing defection and 0 representing cooperation. Then the payoff $U(i, j)$ for the player $M(i, j)$ reads:

$$U(i,j) = \sum_{(k,l)\in I(i,j)} (M(i,j)(M(k,l)P + (1 - M(k,l))T) + (1 - M(i,j))(M(k,l)S + (1 - M(k,l))R)); \quad (1)$$

where $I(i, j)$ is the set of indices of eight closest neighbors of the player $M(i, j)$. The payoff matrix U is used to update the strategy of players in the next time step:

$$\hat{M}(i, j) = M(r, s); \tag{2}$$

where $\hat{M}(i, j)$ is the strategy of the player $M(i, j)$ in the next time step; (r, s) are the coordinates of the neighbor who has previously received the highest payoff:

$$(r, s) = \arg \max_{(k,l)\in I(i,j)\cup\{(i,j)\}} U(k, l). \tag{3}$$

The payoff matrix U is recalculated as soon as strategies for all players are updated.

2.2. The generation of the initial population

The generation of the initial population (the matrix M) is an important step in the proposed communication scheme. A simple solution would be using a dichotomous random number generator to initialize the matrix M. But the Receiver must be able to generate an identical copy of the matrix M (the transfer of the whole matrix of initial conditions from the Sender to the Receiver would be too costly). The logistic map

$$x_{k+1} = ax_k(1 - x_k) \tag{4}$$

generates a chaotic sequence at $a = 4$ and at almost all initial conditions x_0 from the interval $[0; 1]$ [27,28]. The logistic map is successfully used in many image encryption algorithms [29,30]. However, the logistic map has some common weaknesses such as stable windows, a relatively small key space and an uneven distribution of sequences (all these defects may be utilized by the attackers). The intertwined logistic map [31] has been proposed in order to overcome all the weaknesses of the logistic map. Nevertheless, we use the logistic map (it can be easily replaced by the intertwined logistic map, if needed). For example, the uneven distribution of sequences generated by the chaotic logistic map does not make any harm in our computational setup—this distribution is symmetric with respect to 0.5. All numerical values of $x_k < 0.5$ are stored as zeros and $x_k \geq 0.5$ are stored as ones in consecutive elements of matrix M and the initial condition x_0 serves as a key for the Receiver.

2.3. The evolution of patterns

Different parameters of the model (R, S, T, P) result into different evolution of the patterns from the same initial conditions. Fig. 1 shows some typical behavior of the system. The size of the matrix M is 200×200 pixels; each pixel represents an individual player. The initial population is shown in Fig. 1(a). The evolution of the system depends on the parameters of the model. All players do cooperate at $R = 3; S = 1; T = 5; P = 1$ after 30 forward time steps from the initial conditions (Fig. 1(b)). Some players start to defect at $R = 3; S = 0; T = 4; P = 1$ (Fig. 1(c)). Dichotomous patterns are generated at $R = 3; S = 1; T = 5; P = 0$ (Fig. 1(d); most players do cooperate) and at $R = 3; S = 2; T = 4; P = 0$ (Fig. 1(e); most players do defect).

3. The communication scheme based on ESG

Let us consider the following communication algorithm between Bob (the sender) and Alice (the receiver). Bob generates an initial population of players (Fig. 1(a)) and modifies this dichotomous picture by inverting pixels which are located in the regions occupied by the secret image. Then Bob runs the iterative ESG model of the grid for a predetermined number of steps and saves the matrix A. Bob sends this dichotomous image via an open communication channel to Alice. Bob also sends 2 public keys—x_0 (the initial conditions of the logistic map) and N (the number of forward iterations for the ESG model).

Alice knows 4 private keys: $R; S; T; P$. Upon receiving x_0 Alice does generate the unperturbed copy of initial population (the size of the grid is given by the dimensions of the received image from Bob). Then she runs the iterative ESG algorithm on the grid (starting from the unperturbed initial population) for N forward steps. Finally, Alice performs XOR subtraction between her image and the image received from Bob. The difference image should leak the shape of the secret image encoded into the initial population by Bob.

It is clear that such communication algorithm will not work for any set of parameters $R; S; T; P$. Take Fig. 1(b) for example—all players do cooperate after 30 forward iterations and it is impossible to expect that the difference image would reveal any meaningful information. In other words, it is important to define the space of private keys where the communication algorithm is operable.

First of all we define the secret image—it is illustrated in Fig. 2(a). The dichotomous image of perturbed initial conditions is constructed as follows. All pixels are copied from Fig. 1(a) to Fig. 2(b) at positions corresponding to the black color in the secret image. Similarly, inverted copies of pixels from the initial population are copied to Fig. 2(b) at positions corresponding to the white color in the secret image. In other words, Fig. 2(b) is a copy of Fig. 1(a) at all pixels except where the secret image is white (there pixels are inverted).

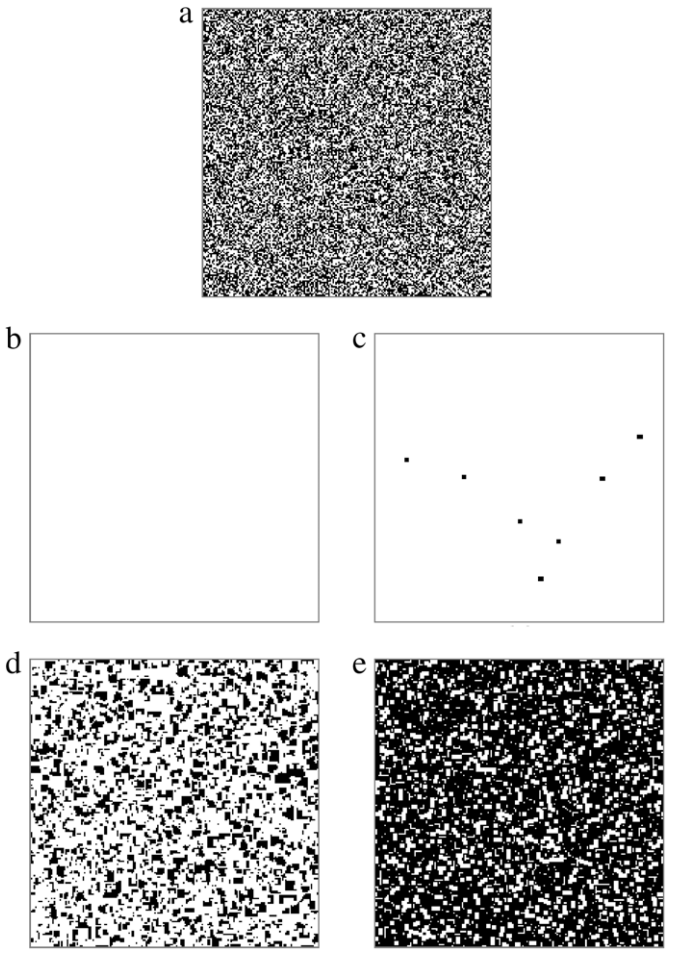

Fig. 1. Typical patterns generated by the iterative ESG model on a grid. Part (a) shows the initial condition. Patterns evolved after 30 steps are illustrated in part (b) (at $R = 3; S = 1; T = 5; P = 1$); part (c) (at $R = 3;\ S = 0; T = 4; P = 1$); part (d) (at $R = 3; S = 1; T = 5; P = 0$) and part (e) (at $R = 3; S = 2; T = 4; P = 0$).

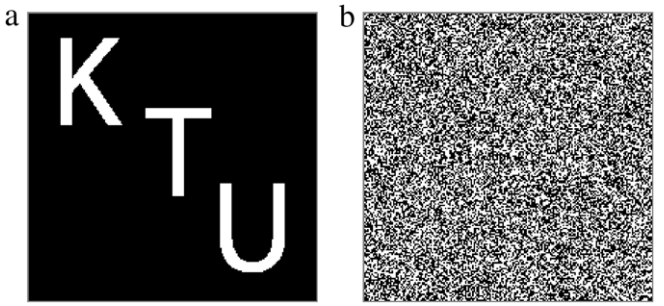

Fig. 2. The secret information (part (a)) and the image of perturbed initial conditions (part (b)).

We do execute the iterative ESG model on the grid for 30 forward iterations starting from Fig. 2(b). The resulting patterns and the difference images are presented in Fig. 3. The set of parameters $R = 3; S = 1; T = 5; P = 1$ yield a plain white image (Fig. 3(a)); the XOR difference image between Fig. 1(b) and Fig. 3(a) is plain black and does not reveal any secret (Fig. 3(b)). Parameters $R = 3; S = 0; T = 4; P = 1$ yield an identical copy of Fig. 1(c)—the difference image is also black (Fig. 3(d)). But parameters $R = 3; S = 1; T = 5; P = 0$ result in a different pattern than Fig. 1(d)—the difference image in Fig. 3(f) is a complex dichotomous image. Unfortunately, it is impossible to read the secret image from Fig. 3(f). Finally, the set of parameters $R = 3; S = 2; T = 4; P = 0$ produces a pattern which results into the difference image which leaks the secret (Fig. 3(h)).

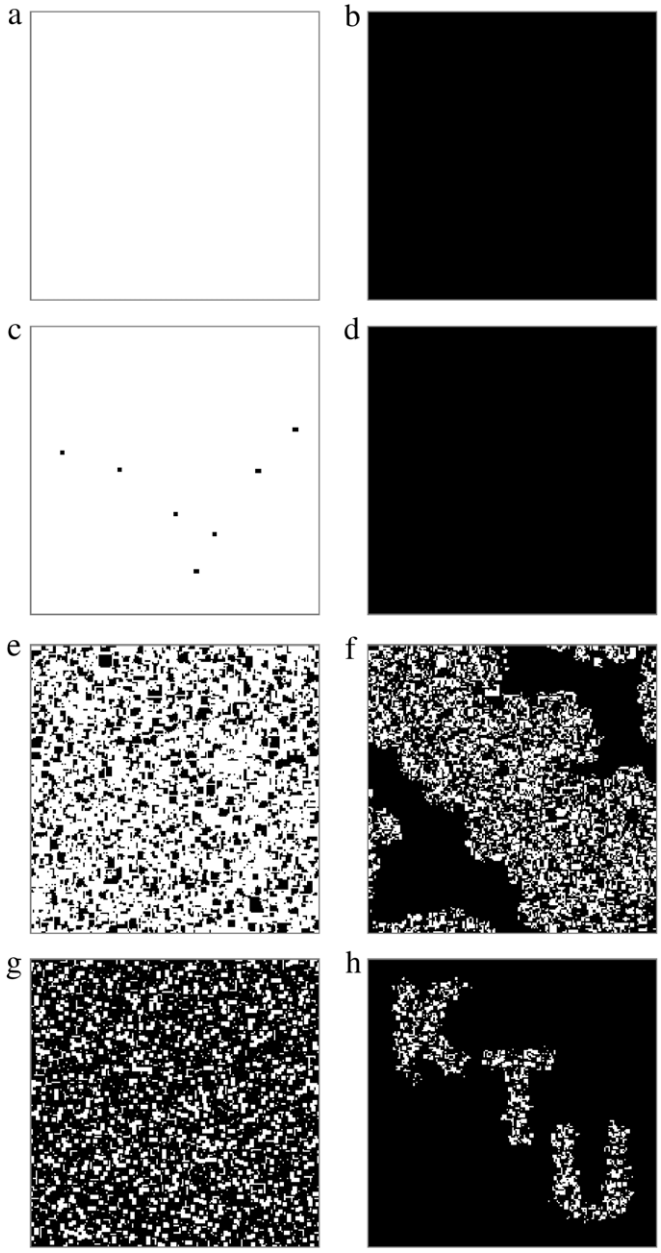

Fig. 3. Patterns (the left column) and difference images (the right column) generated by ESG from the perturbed initial conditions after 30 time forward steps. Parts (a) and (b) correspond to $R = 3; S = 1; T = 5; P = 1$; parts (c) and (d)—to $R = 3; S = 0; T = 4; P = 1$; parts (e) and (f)—to $R = 3; S = 1; T = 5; P = 0$; parts (g) and (h)—to $R = 3; S = 2; T = 4; P = 0$.

4. Properties of the communication system based on ESG

4.1. The minimal size of a detectable element in the secret image

The definition of Nash equilibrium in a multiplayer spatial ESG game implies that an action of one single player in opposite to the equilibrium does not generate a greater individual benefit neither for him nor for the whole community of players compared to the situation which was available in that state of equilibrium. In other words, one may expect that the difference image would be black if the secret image would contain only one single white pixel (at $R = 3; S = 2; T = 4; P = 0$). This fact is demonstrated by the following computation experiment.

Let the whole secret image is black except one pixel which is white (a particular location of the pixel is not important due to periodic boundary conditions). We do invert one pixel in the matrix of initial conditions M; the coordinates of that

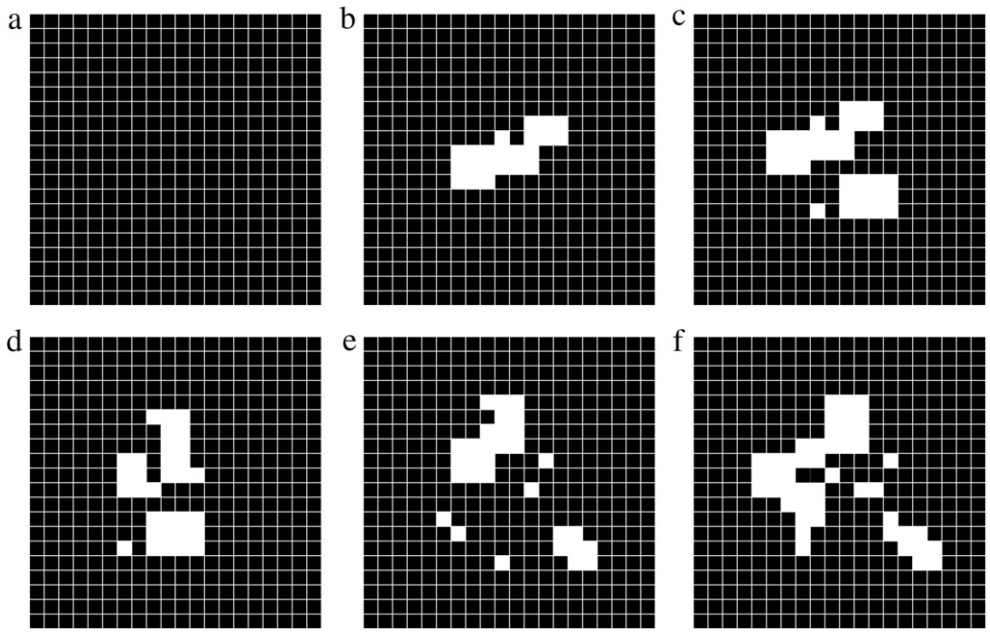

Fig. 4. A single player cannot change the long-term behavior of the system—1 white pixel in the secret image does not yield any changes in the difference image (part (a)). A 2×2 square block of white pixels in the secret image does produce a complex response in the difference image (part (b)). Difference images generated by 3×3, 4×4, 5×5 and 6×6 square blocks of white pixels are shown in parts (c)–(f) accordingly.

pixel corresponds to the coordinates of the white pixel in the secret image (we use the same unperturbed initial conditions as before). 30 time forward steps are executed from the perturbed matrix M; the difference image is shown in Fig. 4(a). We do not show only the zoomed region around the perturbed pixel in Fig. 4(a)—white lines denote boundaries between pixels. It is clear that one player is not able to change the evolution of the whole community of players.

Next we repeat the computation experiment, but the secret image contains one block of white pixels; the size of this block is 2×2. The resultant difference image is shown in Fig. 4(b). It is interesting to note that a synchronized action of a group of players (4 players did invert their strategy in the matrix of initial conditions) results in a different pattern of strategies after 30 time steps. Moreover, the changes in the difference image occupy a region wider than 2×2 pixels.

The situation becomes even more complex when the size of the block of white pixels is 3×3 (Fig. 4(c)). The changes in the difference do occupy a region not only larger than 3×3 pixels this region is not path-connected. The complexity of the difference image grows as the size of the block of white pixels in the secret image increases Fig. 4(d) shows the difference image for 4×4 block; Fig. 4(e)—for 5×5 block; Fig. 4(f)—for 6×6 block.

4.2. The minimum detectable distance between two objects

It can be seen from the results presented in Fig. 4 that changes in the difference image do occupy a region wider than the object originating these changes. A simple visual comparison of Fig. 2(a) and Fig. 3(f) suggests that the pattern of changes in the difference image spreads around the skeleton of the secret image. In that respect such spreading around the contours of the secret image reminds the process of diffusion—though physical principles governing the formation of the difference image are completely different.

This effect of spreading poses a definite constraint for the construction of the secret image. One must take care about the minimal distance between two objects in the secret image which would be detectable as separate objects in the difference image. A computational experiment in Fig. 5 illustrates this effect. We do consider two parallel lines in the secret image (Fig. 5(a)). The width of each of these two lines is 5 pixels (that is more than enough to originate changes in the difference image). The distance between these two lines is increased from 5 pixels (Fig. 5(a)) to 15 pixels (Fig. 5(e)). The difference image originated by Fig. 5(a) does not allow to distinguish two separate lines in the secret image.

4.3. The detectability of inversions in the initial population

A pseudo-randomly generated dichotomous image represents two different strategies. Let us assume that the number of pixels in this image is n and the probability of finding a 0 or 1 is $0.5 \pm \epsilon$ respectively. A region of m elements corresponding to the location of the secret information must be inverted in order to proceed with the communication scheme.

One may assume that the inverted part of the image is not genuinely random if the probability of finding a 0 or 1 is not in the interval $[0.5 - \delta; 0.5 + \delta]$. Note that, the number of zeros (ones) in the original image before the inversion was

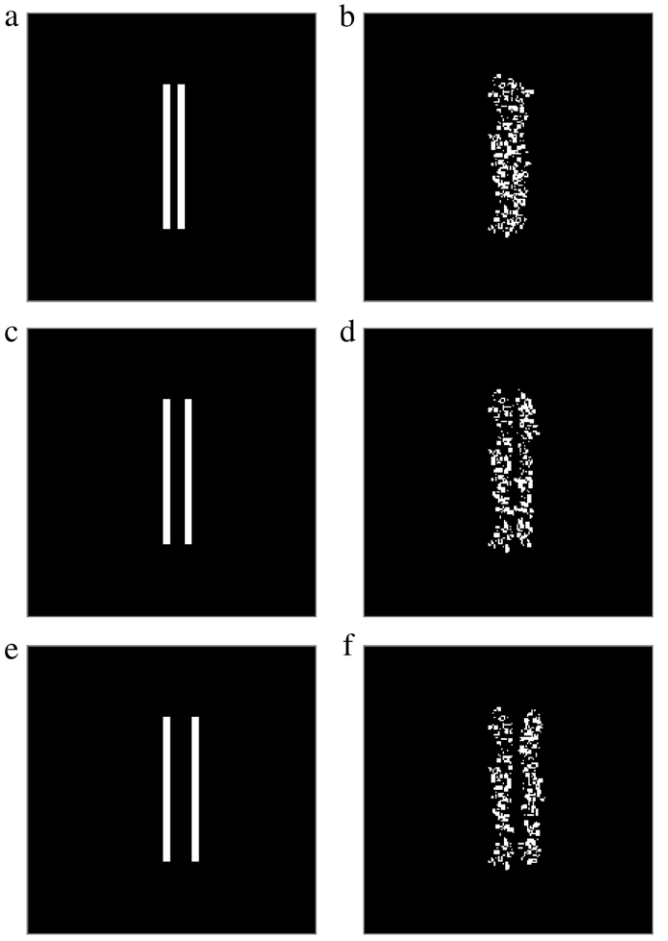

Fig. 5. Two 100×5 primitives (the left column) are separated by 5, 10 and 15 pixels in (a), (c) and (e) respectively. Difference images (the right column) using parameters $R = 3$; $S = 2$; $T = 4$; $P = 0$ are shown in (b), (d) and (f) accordingly.

$(0.5 \pm \epsilon)n$. Without the loss of generality we can state that a freely chosen inversed region originally had k elements of the globally dominant color. Therefore, the whole image after the inversion comprises $(0.5 \pm \epsilon)n \pm (m - 2k)$ different pixels. We do request that the quantity of zeros (ones) must be at least $(0.5 - \delta)n$. The latter requirement yields:

$$\begin{cases} 0.5(m + (\epsilon - \delta)n) \leq k \leq 0.5(m + (\epsilon + \delta)n); \\ 0 \leq k \leq m; \\ k \in Z. \end{cases} \tag{5}$$

The pseudo-randomly generated image must comprise at least m pixels of either color in order for Eq. (5) to hold. Then the probability stating that an element of either color can be found indeed with a probability in the interval $0.5 \mp \delta$ after the modification of the original image reads:

$$P(\epsilon, \delta) = \frac{\sum_k \binom{(0.5+\epsilon)n}{k} \binom{(0.5-\epsilon)n}{m-k}}{\binom{n}{m}}. \tag{6}$$

Fig. 6 illustrates the relationship among $P(\epsilon, \delta)$, ϵ and δ at $n = 100$ and $m = 10$. It can be seen that the inversion of a selected region in the original image is practically undetectable if $\epsilon < 0.1$.

4.4. The sensitivity of the decoding algorithm to the perturbation of private keys

Private keys R, S, T, P play a crucial role in the evolution of the patterns generated by the ESG algorithm. Non-synchronized perturbations of private keys do result in the failure of the communication scheme.

Let us assume that Alice does not know the exact values of private keys. Instead of using $R = 3$; $S = 2$; $T = 4$; $P = 0$ she sets $R = 3.01$; $S = 2$; $T = 4$; $P = 0$. In other words, we do perturb the parameter R—any other parameter (or a combination of parameters) could be perturbed instead.

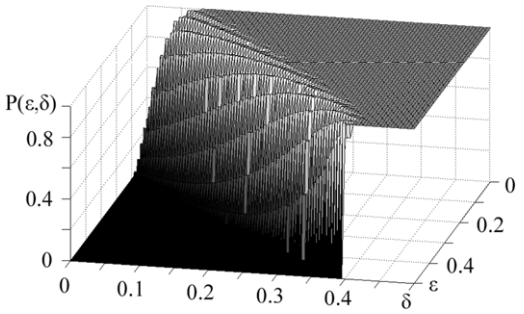

Fig. 6. Probabilities $P(\epsilon, \delta)$ (calculated using Eq. (6)) for the fixed parameters $n = 100$, $m = 10$ and ϵ, δ as variables.

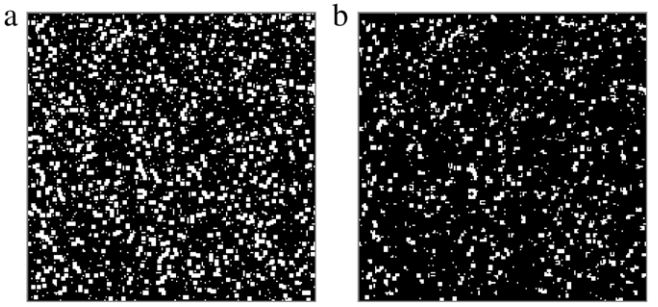

Fig. 7. The sensitivity of the communication scheme on the perturbation of private keys. The pattern produced by $R = 3.01; S = 2; T = 4; P = 0$ from unperturbed initial conditions (Fig. 1(a)) after 30 time forward steps is shown in part (a). The difference image between this pattern and the pattern produced by $R = 3; S = 2; T = 4; P = 0$ from perturbed initial conditions (Fig. 2(b)) after 30 time forward steps does not reveal the secret image (difference is shown in part (b)).

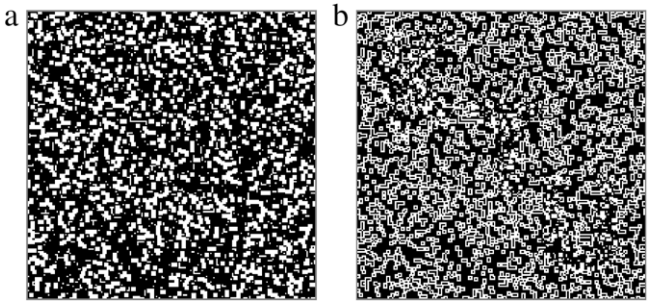

Fig. 8. The sensitivity of the communication scheme on the perturbation of the public key N. The pattern produced by $R = 3; S = 2; T = 4; P = 0$ from unperturbed initial conditions (Fig. 1(a)) after 31 time forward steps is shown in part (a). The difference image between this pattern and the pattern produced by $R = 3; S = 2; T = 4; P = 0$ from the perturbed initial conditions (Fig. 2(b)) after 30 time forward steps (Fig. 3(g)) does not reveal the secret image (the difference is shown in part (b)).

Let us assume that Alice has received a pattern (Fig. 3(g)) from Bob—this pattern has been evolved from the perturbed initial conditions (Fig. 2(b)) after 30 time forward iterations at $R = 3; S = 2; T = 4; P = 0$. Alice does have the correct values of public keys x_0 and N. She does generate the correct copy of unperturbed initial conditions (Fig. 1(a)) and does execute the ESG algorithm for 30 time forward steps. The only problem is that Alice uses $R = 3.01$ instead of $R = 3$. The pattern produced by Alice is shown in Fig. 7(a). The XOR difference image between Fig. 3(g) and Fig. 7(a) is shown in Fig. 7(b). There is no way Alice could interpret the secret image from the difference image.

It can be noted that an abbreviate selection of private keys R, S, T, P does not result in a functional communication system as demonstrated in Fig. 3—only small perturbations around $R = 3; S = 2; T = 4; P = 0$ ensure a satisfactory operability of the system. The applicable range of private keys in our experiment is $R = 3 \pm 0.1; S = 2 \pm 0.1; T = 4 \pm 0.1; P = 0 \pm 0.1$.

4.5. The sensitivity of the decoding algorithm to the perturbation of public keys

Let us assume that Bob and Alice know correct private keys ($R = 3; S = 2; T = 4; P = 0$), the correct initial condition x_0 ($x_0 = 0.01$) but Alice uses $N = 31$ instead of 30. Fig. 8(a) shows the pattern produced by unperturbed initial conditions

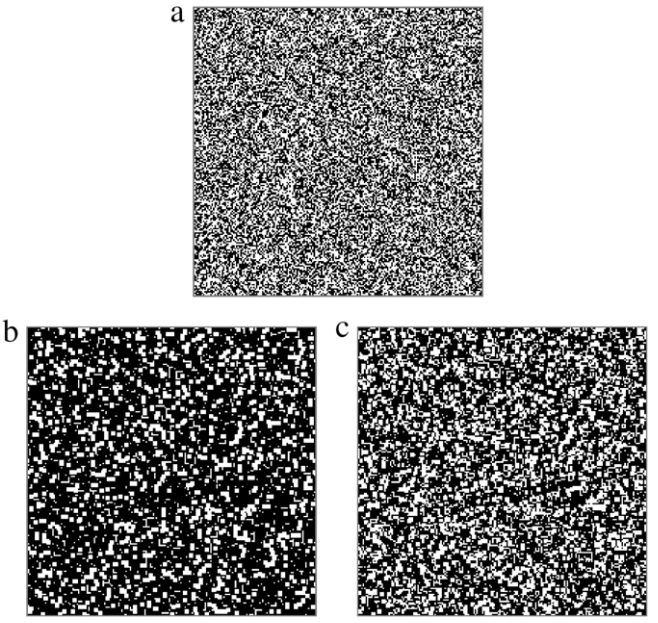

Fig. 9. The sensitivity of the communication scheme on the perturbation of the public key x_0. The unperturbed initial state generated using Eq. (4) and $x_0 = 0.0101$ is shown in part (a). The pattern produced by $R = 3; S = 2; T = 4; P = 0$ from unperturbed initial conditions (a) after 30 time forward steps is shown in part (b). The difference image between this pattern and the pattern produced by $R = 3; S = 2; T = 4; P = 0$ from the perturbed initial conditions (Fig. 2(b)) after 30 time forward steps (Fig. 3(g)) does not reveal the secret image (the difference is shown in part (c)).

after 31 time forward steps. The difference image between Fig. 8(a) and the transmitted pattern Fig. 3(g) results into an uninterpretable image shown in Fig. 8(b).

The selection of N is determined by the length of the transient processes in the evolutionary spatial 2×2 game. Too small values of N do not result in a well-developed pattern and could not be used for the transmission of the secret information. The size of the grid does have a definite impact on the formation of patterns as well—a grid being able to accommodate only few primitives of the pattern (as illustrated in Fig. 4) cannot be exploited for the proposed communication system. Both the size of the grid and the number of time steps must be large enough for the formation of a well-developed pattern sensitive to initial perturbations. In fact, the applicable range of N does not depend on the size of the grid if it is large enough (more than 100×100 in our experiments) and N is also large enough (more than 20 in our experiments).

Now let us assume that Bob and Alice know correct private keys, the correct value of N, but Alice uses a slightly different value of x_0 ($x_0 = 0.0101$). The pattern generated by Alice from unperturbed initial conditions (Fig. 9(a)) after 30 time forward steps is shown in Fig. 9(b). The difference image between Fig. 9(a) and Fig. 3(g) does not reveal the secret image (Fig. 9(c)). A slight perturbation of x_0 generates a completely different image of unperturbed initial conditions (compare Fig. 9(a) to Fig. 1(a)) due to the chaotic properties of the logistic map.

4.6. The impossibility of a time-backwards step

The pattern produced by the ESG algorithm from perturbed initial conditions is transmitted via an open communication channel. Let us assume that an eavesdropper is able to capture a copy of the transmitted image. Moreover, let us assume that he also does know the private keys (R, S, T, P)—but he does not know the unperturbed initial conditions (he cannot construct the pattern from the unperturbed initial conditions and cannot compute the XOR difference image).

It is important to make sure that the ESG algorithm does not allow a time-backward step. Let us assume that $M(i, j)$ is the strategy of the ith-jth player after N forward time steps. The computation of the payoffs for his surrounding neighbors at the current time step is a straightforward procedure according to Eq. (1). But the eavesdropper needs to know payoffs of all 8 neighbors of $M(i, j)$ in the previous time step in order to make a step backwards in time. In its turn, payoffs in the previous time step can be computed only if the strategies of all players are known in the previous time step as shown in Fig. 10. That leads to a contradiction which does not allow a time backward iteration.

4.7. The plain image attack

Let us assume that Bob and Alice know all private and public keys. One could consider a situation when unperturbed initial conditions are assumed as a plain image—be it a fault of the pseudo-random number generator, or a plain image attack from an eavesdropper. As mentioned in introduction, the logistic map cannot be considered as a good random number generator

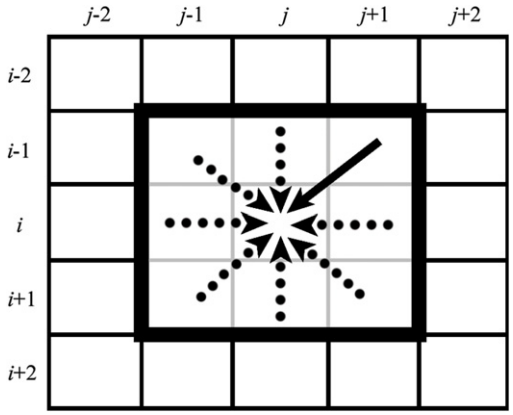

Fig. 10. Illustration representing the fact that it is a straightforward computation (according to Eq. (1)) using 8 immediate neighbors that leads to the time forward step—yet only one adjacent strategy (illustrated by a thick solid arrow) is selected afterwards.

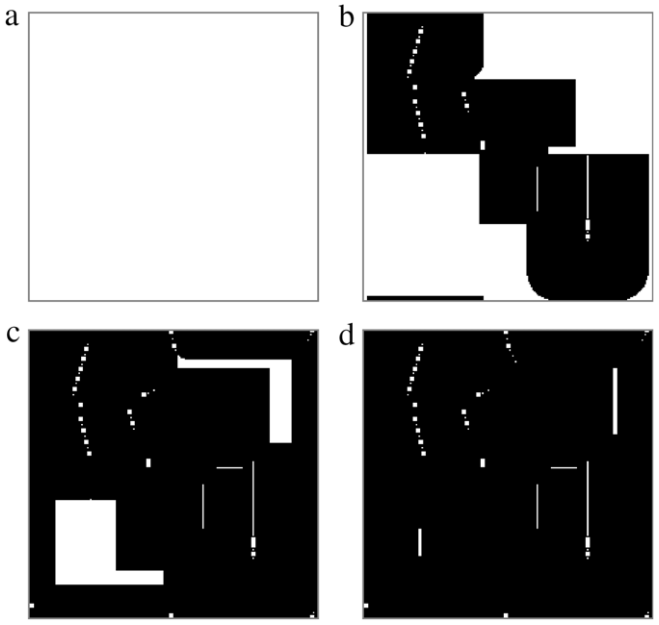

Fig. 11. Patterns produced by parameters $R = 3$; $S = 2$; $T = 4$; $P = 0$. Evolution of plain white image after 20 time forward steps is shown in part (a). Evolution of XOR difference between part (a) and Fig. 2(a) after 20, 40, 60 time forward steps is shown in part (b), (c), (d) respectively.

for all values of x_0. Let us take an example when $x_0 = 3/4$, then $x_k = 3/4$ for all $k \geq 0$. The image of unperturbed initial conditions will be a white plain. This is a stationary state for the ESG algorithm at $R = 3; S = 2; T = 4; P = 0$; the produced image after 20 time forward steps is shown in Fig. 11(a). The evolution of patterns produced by the perturbed initial conditions is shown in Fig. 11 part (b) (after 20 time forward iterations), part (d) (after 40 time forward iterations), part (d) (after 60 time forward iterations).

It is clear that the proposed communication system is resilient to a plain image attack—Alice cannot generate any pattern at all while Bob's image is an undeveloped pattern.

5. An illustrative example and concluding remarks

A proper selection of system's parameters offers an excellent functionality of the proposed communication system. Patterns generated by the ESG model are able to reproduce and to transmit secure images: Fig. 12 shows a realistic communication scenario (the gray shaded area represents the actions of Bob; the area surrounded by the thick dotted line represents the actions of Alice). Bob and Alice must start from the same initial conditions, but Bob does perturb these initial conditions by inverting pixels in the zones corresponding to the secret image. Alice does not know the secret image—she simply uses ESG algorithm to produce the pattern from unperturbed initial conditions. XOR difference between Alice's and Bob's patterns leaks the secret (Fig. 12).

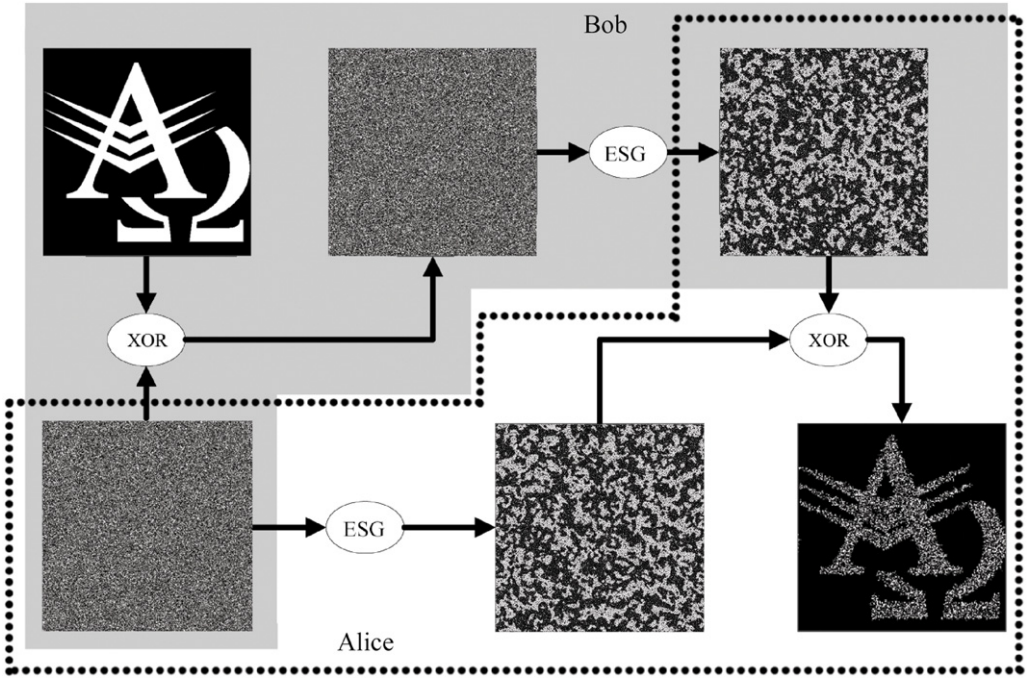

Fig. 12. Bob and Alice starts from the same initial conditions (lower left), but Bob does perturb these initial conditions by inverting pixels in the zones corresponding to the secret image (upper left). Alice does not know the secret image—she simply uses ESG algorithm to produce the pattern from unperturbed initial conditions. XOR difference between Alice's and Bob's patterns leaks the secret (lower right).

The described way of obtaining the relevant self-organizing patterns has some convenient properties. We do not need to generate additional representations of the original secret image (given that it is already black–white) or to perturb initial conditions by adding artificial values to the present states of discrete pixels (as it is performed in Ref. [17]). We simply invert dichotomous pixels in the regions corresponding to the secret image. Nevertheless, the storage capacity of the proposed communication scheme is comparable to the one presented in Ref. [17]—the minimum distance between two primitives is 10 pixels in the proposed scheme (Fig. 5) while it is 15 pixels in the system presented in Ref. [17].

The proposed communication algorithm exploits cooperation between competing individuals for hiding secret visual information into self-organizing patterns. We have used a basic 2×2 game without memory and without more complex stochastic spatial interaction rules between adjacent players. We did not specify the 2×2 game; the functionality of the system is determined by the proper selection of parameters R, S, T, P which guarantee not only the formation of well-developed spatial patterns, but also their sensitivity to small perturbations. Nevertheless, the physical principles of the formation of patterns in the proposed communication scheme are different from the system presented in Ref. [17]. We do employ not a predator–prey model with self- and cross-diffusion but an evolutionary spatial 2×2 game. This changes the perturbation, transmission and decoding procedures completely. More sophisticated ESG models could be used in similar communication schemes (what is a definite objective for future research). Nevertheless, patterns induced by basic evolutionary models of competition and cooperation can be successfully used for the secure encryption and transmission of secret digital images.

Acknowledgment

Financial support from the Lithuanian Science Council under project No. MIP-100/12 is acknowledged.

References

[1] Martin A. Nowak, Robert M. May, Evolutionary games and spatial chaos, Nature 359 (6398) (1992) 826–829.
[2] R.M. Axelrod, The Evolution of Cooperation, Basic Books, New York, 2006.
[3] J. Hofbauer, K. Sigmund, Evolutionary Games and Population Dynamics, Cambridge University Press, Cambridge, 1998.
[4] Matjaž Perc, Attila Szolnoki, Coevolutionary games—a mini review, Biosystems 99 (2) (2010) 109–125.
[5] György Szabó, Gábor Fáth, Evolutionary games on graphs, Phys. Rep. 446 (4) (2007) 97–216.
[6] Matjaž Perc, Jesús Gómez-Gardeñes, Attila Szolnoki, Luis M Floría, Yamir Moreno, Evolutionary dynamics of group interactions on structured populations: a review, J. R. Soc. Interface 10 (80) (2013).
[7] Ping-Ping Li, Jianhong Ke, Zhenquan Lin, P.M. Hui, Cooperative behavior in evolutionary snowdrift games with the unconditional imitation rule on regular lattices, Phys. Rev. E 85 (2) (2012) 021111.

[8] Keizo Shigaki, Jun Tanimoto, Zhen Wang, Satoshi Kokubo, Aya Hagishima, Naoki Ikegaya, Referring to the social performance promotes cooperation in spatial prisoner's dilemma games, Phys. Rev. E 86 (3) (2012) 031141.
[9] Zhaojin Xu, Haizhao Zhi, Lianzhong Zhang, Survival via cooperation in the prisoner's dilemma game, Phys. Rev. E 84 (5) (2011) 051114.
[10] György Szabó, Attila Szolnoki, Melinda Varga, Lívia Hanusovszky, Ordering in spatial evolutionary games for pairwise collective strategy updates, Phys. Rev. E 82 (2) (2010) 026110.
[11] Simo Heliövaara, Harri Ehtamo, Dirk Helbing, Timo Korhonen, Patient and impatient pedestrians in a spatial game for egress congestion, Phys. Rev. E 87 (1) (2013) 012802.
[12] Attila Szolnoki, Matjaž Perc, Impact of critical mass on the evolution of cooperation in spatial public goods games, Phys. Rev. E 81 (5) (2010) 057101.
[13] György Szabó, Attila Szolnoki, Cooperation in spatial prisoner's dilemma with two types of players for increasing number of neighbors, Phys. Rev. E 79 (2009) 016106.
[14] Masaki Tomochi, Mitsuo Kono, Spatial prisoner's dilemma games with dynamic payoff matrices, Phys. Rev. E 65 (2002) 026112.
[15] Pierre Buesser, Marco Tomassini, Evolution of cooperation on spatially embedded networks, Phys. Rev. E 86 (6) (2012) 066107.
[16] Qionglin Dai, Hongyan Cheng, Haihong Li, Yuting Li, Mei Zhang, Junzhong Yang, Crossover between structured and well-mixed networks in an evolutionary prisoner's dilemma game, Phys. Rev. E 84 (1) (2011) 011103.
[17] Loreta Saunoriene, Minvydas Ragulskis, Secure steganographic communication algorithm based on self-organizing patterns, Phys. Rev. E 84 (5 Pt 2) (2011) 056213.
[18] H. Fort, E. Sicardi, Evolutionary Markovian strategies in 2 × 2 spatial games, Physica A 375 (2007) 323–335.
[19] M. Dresher, The Mathematics of Games of Strategy: Theory and Applications, in: Dover Books on Mathematics Series, Dover, 1981.
[20] A. Rapoport, A.M. Chammah, Prisoner's Dilemma: A Study in Conflict and Cooperation, University of Michigan Press, Michigan, 1965.
[21] Matjaž Perc, Zhen Wang, Heterogeneous aspirations promote cooperation in the prisoner's dilemma game, PLoS One 5 (12) (2010) e15117.
[22] Stephen Le, Robert Boyd, Evolutionary dynamics of the continuous iterated prisoner's dilemma, J. Theoret. Biol. 245 (2) (2007) 258–267.
[23] B. Skyrms, The Stag Hunt and the Evolution of Social Structure, Cambridge University Press, Cambridge, 2004.
[24] J. Maynard Smith, G.R. Price, The logic of animal conflict, Nature 246 (5427) (1973) 15–18.
[25] Frank Emmert-Streib, Exploratory analysis of spatiotemporal patterns of cellular automata by clustering compressibility, Phys. Rev. E 81 (2 Pt 2) (2010) 026103.
[26] Stephen Wolfram, Statistical mechanics of cellular automata, Rev. Modern Phys. 55 (3) (1983) 601–644.
[27] Robert M. May, et al., Simple mathematical models with very complicated dynamics, Nature 261 (5560) (1976) 459–467.
[28] P. Collet, J.P. Eckmann, Iterated Maps on the Interval as Dynamical Systems, Modern Birkhäuser classics, Boston, 2009.
[29] Narendra K. Pareek, Vinod Patidar, Krishan K. Sud, Image encryption using chaotic logistic map, Image Vis. Comput. 24 (9) (2006) 926–934.
[30] Ahmed A. Abd El-Latif, Li Li, Ning Wang, Qi Han, Xiamu Niu, A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, Signal Process. 93 (11) (2013) 2986–3000.
[31] Xingyuan Wang, Dapeng Luan, A novel image encryption algorithm using chaos and reversible cellular automata, Commun. Nonlinear Sci. Numer. Simul. 18 (11) (2013) 3075–3085.