



On the bifurcation of Marotto's map and its application in image encryption



S.M. Salman^{a,*}, A.A. Elsadany^b

^a Faculty of Education, Alexandria University, Alexandria, Egypt

^b Basic Science Department, Faculty of Computers and Informatics, Suez Canal University, Ismailia 41522, Egypt

ARTICLE INFO

Article history:

Received 13 April 2017

Received in revised form 29 June 2017

MSC 2010:

37E10

37C75

34C28

Keywords:

Marotto's map

Stability

Bifurcation

Compound chaos

Spatiotemporal chaos

Image encryption

ABSTRACT

The aim of this paper is to address the codimension-one bifurcation of Marotto's map and its utility in image encryption. First of all, local stability analysis and local bifurcation analysis of fixed points of the considered map are investigated in details. According to the classical bifurcation theory and the center manifold theorem, the map exhibits various bifurcation types such as transcritical, flip and Neimark–Sacker bifurcations. Second of all, the map is proven to be chaotic in the sense of Marotto. Since image encryption based on chaotic maps is very promising for cryptography, Marotto's map, compound chaos, and spatiotemporal chaos are combined to encrypt and decrypt images. Numerical simulations agree with the analytical framework for the complex dynamics of the map. Furthermore, different test images are used to demonstrate the effectiveness of the method implemented for encryption.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

The study of nonlinear difference equations has gained a great interest in the past decades because they can display variety of complex dynamic behavior such as different types of bifurcations, periodic orbits and chaotic attractors [1–9]. Indeed, the defining equations of many nonlinear systems have parameters and the question is how the dynamic behavior is changed when changing these parameters [10]. Two-dimensional maps have been used for modeling mathematical equations which describe certain dynamical process [11]. In many fields like imaging, digital filtering, and spatiotemporal chaos, two-dimensional maps have been a focused area of investigation [12–20]. For detailed bifurcation analysis for two-dimensional maps, one can see [21–24].

In the present paper, we investigate in details the dynamic behavior of the Marotto's map [25] given by the following discrete-time dynamical system

$$\begin{aligned} x_{n+1} &= (ax_n + by_n)(1 - ax_n - by_n), \\ y_{n+1} &= x_n, \end{aligned} \quad (1.1)$$

where the control parameters a and b are restricted to be in the region

$$Q = \{(a, b) : a, b \geq 0, a + b \leq 4\}.$$

* Corresponding author.

E-mail addresses: samastars9@gmail.com (S.M. Salman), aelsadany1@yahoo.com (A.A. Elsadany).

The definition of discrete chaos was first introduced in 1975 by Li and Yorke [26] when they put a chaos criteria in one-dimensional difference equations. Afterwards, Marotto generalized the result to n -dimensional difference equations in 1978 and showed that the existence of a snap-back repeller implies chaos in the sense of Li–Yorke [25].

Map (1.1) is known as Marotto's map and actually it has no physical or biological meaning. Nevertheless, it can be used in image encryption which is considered as one of the different ways used to ensure security for images as a result of the ever increasing gross of multimedia applications. Due to intrinsic futures of images such as huge data capacity and high redundancy, classical image encryption such as RSA, AES, DES and IDEA [27,28] are not effective anymore. Therefore, a lot of encryption methods have been introduced or developed to overcome the image encryption problems related to classical methods. Recently, cryptography based on chaotic systems have attracted the attention of many researches because of their important properties such as sensitive dependence on initial conditions, aperiodicity, and unpredictability which can satisfy the requirements such as diffusion and mixing in the sense of cryptography [29–45]. Chaotic maps may be classified into two categories: one-dimensional and higher-dimensional. The first type of maps have simple structures and simple chaotic orbits and can be easily predicted. Thus image encryption using one-dimensional chaotic maps are insecure [46–49]. On the contrary, higher-dimensional chaotic maps have more complex structure and complex chaotic performance which make prediction of their chaotic orbits is harder. In [50], an image encryption method based on the two-dimensional logistic map was proposed, however, this method is not effective in cryptography because the key length is not sufficient, not secure, and encryption time is high [51]. To overcome these drawbacks, high-dimensional chaotic maps are used in image encryption because of their strong features such as large number of Lyapunov exponents and longer aperiodicity [52]. On the other hand, spatiotemporal chaotic maps have been employed in cryptography as they have more complex dynamics and high unpredictability [53–56].

In this paper, we adopt the encryption method presented in [57] in which a Hénon map and compound spatiotemporal chaos were employed. We will replace the Hénon map with the Marotto's map in the positions permutation process while spatiotemporal chaos and compound chaos are combined in the value shuffling process.

The paper is structured as follows. Section 2 discusses existence and local stability of fixed points. In Section 3, local bifurcations analysis of fixed points are studied. Section 4 demonstrates the existence of a snap-back repeller in the sense of Marotto. Section 5 illustrates some numerical simulations for the complex dynamics of the map. In Section 6, we present the encryption method based on Marotto's map and spatiotemporal chaos and compound chaos. Finally, we conclude in Section 7.

2. Existence and local stability of fixed points

System (1.1) has at most two fixed points:

1. For all parameters values there exists one fixed point, namely $\text{fix}_1 = (0, 0)$,
2. For $a + b \neq 1$, there exists an interior fixed point $\text{fix}_2 = (\frac{a+b-1}{(a+b)^2}, \frac{a+b-1}{(a+b)^2})$.

Lemma 1 ([58]). Let $F(\lambda) = \lambda^2 + P\lambda + Q$. Suppose that $F(1) > 0$, and $F(\lambda) = 0$ has two roots λ_1 and λ_2 . Then

1. $F(-1) > 0$ and $Q < 1$ if and only if $|\lambda_1| < 1$ and $|\lambda_2| < 1$;
2. $F(-1) < 0$ if and only if $|\lambda_1| < 1$ and $|\lambda_2| > 1$ (or $|\lambda_1| > 1$ and $|\lambda_2| < 1$);
3. $F(-1) > 0$ and $Q > 1$ if and only if $|\lambda_1| > 1$ and $|\lambda_2| > 1$;
4. $F(-1) = 0$ and $P \neq 0, 2$ if and only if $\lambda_1 = -1$ and $|\lambda_2| \neq 1$;
5. $P^2 - 4Q < 0$ and $Q = 1$ if and only if λ_1 and λ_2 are complex and $|\lambda_{1,2}| = 1$.

The Jacobian matrix calculated at (x^*, y^*) reads

$$J(x^*, y^*) = \begin{pmatrix} a - 2a^2x^* - 2aby^* & -2abx^* + b - 2b^2y^* \\ 1 & 0 \end{pmatrix}.$$

3. Local bifurcations analysis

In this section, a detailed bifurcation analysis is being performed at the fixed points of system (1.1).

Proposition 1. The fixed point $\text{fix}_1 = (0, 0)$ is

1. a sink if:
 - (i) $a > b - 1$, and (ii) $b > 0$,
2. a source if $a > b - 1$,
3. a saddle if $a < b - 1$,
4. a non-hyperbolic if one of the following conditions holds true:
 - (i) $a = 1 - b$ or (ii) $a = b - 1$.

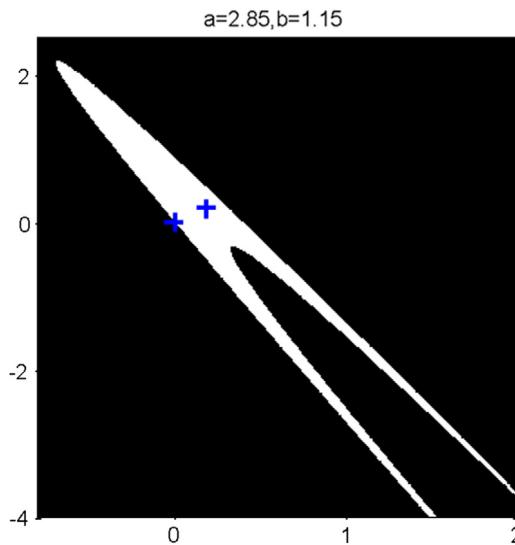


Fig. 1. Basin of attraction of fixed points of Marotto's map (1.1). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Proposition 2. The fixed point $\text{fix}_2 = (\frac{a+b-1}{(a+b)^2}, \frac{a+b-1}{(a+b)^2})$ is

1. a sink if:
(i) $(b - \frac{1}{2})^2 > (a - \frac{3}{2})^2 - 2$ and (ii) $b^2 - 3b < a(1 - b)$,
2. a source if the following conditions are satisfied:
(i) $(b - \frac{1}{2})^2 > (a - \frac{3}{2})^2 - 2$ and (ii) $b^2 - 3b > a(1 - b)$,
3. a saddle if $(b - \frac{1}{2})^2 < (a - \frac{3}{2})^2 - 2$,
4. a non-hyperbolic if:

$$\begin{aligned} \text{(i)} \quad & b = \frac{1}{2} + \sqrt{(a - \frac{3}{2})^2 - 2} \text{ or,} \\ \text{(ii)} \quad & b = \frac{1}{2} - \sqrt{(a - \frac{3}{2})^2 - 2}, \text{ and } a \neq 0, 2 - b, 2 + \sqrt{b(2 - a) + 4}. \end{aligned}$$

Fig. 1 shows the basin of attraction of fixed points of map (1.1) for $b = 1.15$ and $a = 2.85$ in which the fixed points are the two blue crosses at $(0, 0)$ and $(0.1875, 0.1875)$.

3.1. Bifurcation of $\text{fix}_1(0, 0)$

The Jacobian matrix at $\text{fix}_1(0, 0)$ reads

$$J(\text{fix}_1) = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}.$$

First we discuss the occurrence of a transcritical bifurcation at $\text{fix}_1(0, 0)$ in the following lemma.

Lemma 2. If $a = 1 - b$, and $b \neq -1, 1$, then system (1.1) admits a transcritical bifurcation at $\text{fix}_1(0, 0)$.

Proof. Let $a = 1 - b$, the two eigenvalues associated to the Jacobian matrix evaluated at $\text{fix}_1(0, 0)$ become $\lambda_1 = 1$ and $\lambda_2 = -b$. Let $\mu = a - 1 + b$ be a new and a dependent variable, the system (1.1) is transformed into the following form

$$\begin{pmatrix} x \\ y \\ \mu \end{pmatrix} \rightarrow \begin{pmatrix} -b + 1 & b & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ \mu \end{pmatrix} + \begin{pmatrix} \mu x - (\mu - b + 1)^2 x^2 - 2b(\mu - b + 1)xy - b^2 y^2 \\ 0 \\ 0 \end{pmatrix}. \quad (3.1)$$

Constructing an invertible matrix

$$T = \begin{pmatrix} 1 & 0 & -b \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

and using the translation

$$\begin{pmatrix} x \\ y \\ \mu \end{pmatrix} = T \begin{pmatrix} u \\ v \\ \mu_1 \end{pmatrix},$$

the system (1.1) becomes

$$\begin{pmatrix} u \\ v \\ \mu_1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u \\ v \\ \mu_1 \end{pmatrix} + \begin{pmatrix} \phi(u, v, \mu_1) \\ \psi(u, v, \mu_1) \\ 0 \end{pmatrix}, \quad (3.2)$$

where

$$\begin{aligned} \phi(u, v, \mu_1) &= \frac{1}{(1+b)}(\mu_1(u - bv) + (\mu_1 + 1)^2 u^2 \\ &\quad - b^2(\mu_1 - b)^2 v^2 + (2b(\mu_1 - b + 1)^2 - 2(\mu_1 - b + 1)b^2 - 2(\mu_1 - b + 1)b - 2b^2)uv), \\ \psi(u, v, \mu_1) &= \frac{-1}{(1+b)}(\mu_1(u - bv) + (\mu_1 + 1)^2 u^2 \\ &\quad - b^2(\mu_1 - b)^2 v^2 + (2b(\mu_1 - b + 1)^2 - 2(\mu_1 - b + 1)b^2 - 2(\mu_1 - b + 1)b - 2b^2)uv). \end{aligned}$$

Then, according to the center manifold theorem [59], there exists a center manifold for (3.2) which can be given by:

$$W^c(P_1) = \{(u, v, \mu_1) \in \mathbb{R}^3 | v = h(u, \mu_1), h(0, 0) = Dh(0, 0), |u| < \epsilon, |\mu_1| < \hat{\delta}_1\},$$

where $\epsilon, \hat{\delta}_1$ are sufficiently small.

To compute the center manifold W^c we assume

$$v = h(u, \mu_1) = c_0 u^2 + c_1 u \mu_1 + c_2 \mu_1^2 + O((|u| + |\mu_1|)^3), \quad (3.3)$$

where $O((|u| + |\mu_1|)^3)$ is the sum of all terms whose order is great than 2.

The center manifold must satisfy the relation

$$h(u + \phi(u, h(u, \mu_1), \mu_1), \mu_1) = -bh(u, \mu_1) + \psi(u, h(u, \mu_1), \mu_1). \quad (3.4)$$

Substituting (3.3) into (3.4), then equating the like powers' coefficients in (3.4), we obtain

$$c_0 = \frac{(a+b)^2}{(1+b)^2}, \quad c_1 = 1, \quad c_2 = 0.$$

Finally, the map (3.2) restricted to the center manifold will be in the form

$$\begin{aligned} F_2 : u_{n+1} &= \left(1 + \frac{\mu_1}{b+1}\right)u + \frac{-b}{b+1}\mu_1^2 u + \frac{1}{b+1}(-b\mu_1 c_0 - \mu_1 - 1 - b^2(\mu - b)^2 \mu_1 + \mu_1 A)u^2 \\ &\quad + \frac{1}{b+1}(-2b^2(\mu_1 - b)^2 c_0 \mu_1 + c_0 A)u^3 - b^2(\mu_1 - b)^2 c_0^2 u^4 + O((|u| + |\mu_1|)^6), \end{aligned} \quad (3.5)$$

where $A = 2(\mu_1 - b + 1)^2 b - 2(\mu_1 - b + 1)b^2 - 2(\mu_1 - b + 1)b - 2b^2$.

Since we have $F_2(0, 0) = 0$, $\left(\frac{\partial^2 F_2}{\partial \mu_1 \partial u}\right)_{(0,0)} = \frac{6c_0 A}{b+1} \neq 0$, and $\left(\frac{\partial^2 F_2}{\partial^2 u}\right)_{(0,0)} = \frac{-1}{b+1} \neq 0$, then, the system (1.1) undergoes a transcritical bifurcation at $\text{fix}_1(0, 0)$. \square

Now we discuss the possibility of the occurrence of flip bifurcation of $\text{fix}(0, 0)$. The Jacobian matrix $J(0, 0)$ of system (1.1) has two eigenvalues $\lambda_{1,2} = \frac{a \pm \sqrt{a^2 + 4b}}{2}$. If $a = b - 1$, then we have $\lambda_1 = -1, \lambda_2 = b$ with $|\lambda_2| \neq 1$ provided that $b \neq -1, 1$.

Lemma 3. If $a = b - 1$, and $b \neq -1, 1, \frac{3 \pm \sqrt{5}}{2}$, then system (1.1) admits a flip bifurcation at $\text{fix}_1(0, 0)$. In addition, the stable periodic-2 orbit bifurcates from this fixed point.

Proof. Let $a = b - 1$, the two eigenvalues associated to the Jacobian matrix evaluated at $\text{fix}_1(0, 0)$ become $\lambda_1 = -1$ and $\lambda_2 = b$. Let $\mu = a - b + 1$ be a new and a dependent variable, the system (1.1) is transformed into the following form

$$\begin{pmatrix} x \\ y \\ \mu \end{pmatrix} \rightarrow \begin{pmatrix} b-1 & b & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ \mu \end{pmatrix} + \begin{pmatrix} \mu x - (\mu + b - 1)x^2 - 2b(\mu + b - 1)xy - b^2y^2 \\ 0 \\ 0 \end{pmatrix}. \quad (3.6)$$

Constructing an invertible matrix

$$T = \begin{pmatrix} -1 & 0 & b \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

and using the translation

$$\begin{pmatrix} x \\ y \\ \mu \end{pmatrix} = T \begin{pmatrix} u \\ v \\ \mu_1 \end{pmatrix},$$

then the system (3.6) becomes

$$\begin{pmatrix} u \\ v \\ \mu_1 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} u \\ v \\ \mu_1 \end{pmatrix} + \begin{pmatrix} f(u, v, \mu_1) \\ g(u, v, \mu_1) \\ 0 \end{pmatrix}, \quad (3.7)$$

where

$$\begin{aligned} f(u, v, \mu_1) &= \frac{-1}{(1+b)}(\mu(-u + bv) + (-\mu + 2b\mu - 3b + b^2 + 1)u^2 \\ &\quad + (-\mu - 2b^2\mu - 2b^3 + b^2 - b + 1)v^2 + (4b\mu - 2b - 2\mu b^2 - 2b^3)uv), \\ g(u, v, \mu_1) &= \frac{1}{(1+b)}(\mu(-u + bv) + (-\mu + 2b\mu - 3b + b^2 + 1)u^2 \\ &\quad + (-\mu - 2b^2\mu - 2b^3 + b^2 - b + 1)v^2 + (4b\mu - 2b - 2\mu b^2 - 2b^3)uv). \end{aligned}$$

Then, according to the center manifold theorem there exists a center manifold for (3.7) which can be given by:

$$W^c(P_1) = \{(u, v, \mu_1) \in \mathbb{R}^3 | v = h(u, \mu_1), h(0, 0) = Dh(0, 0), |u| < \epsilon, |\mu_1| < \hat{\delta}_1\},$$

where $\epsilon, \hat{\delta}_1$ are sufficiently small.

To compute the center manifold W^c we assume

$$v = h(u, \mu_1) = a_0u^2 + a_1u\mu_1 + a_2\mu_1^2 + O((|u| + |\mu_1|)^3), \quad (3.8)$$

where $O((|u| + |\mu_1|)^3)$ is the sum of second order terms.

The following relation should be satisfied by the center manifold

$$h(-u + f(u, h(u, \mu_1), \mu_1), \mu_1) = bh(u, \mu_1) + g(u, h(u, \mu_1), \mu_1). \quad (3.9)$$

Substituting (3.8) into (3.9), then equating like powers' coefficients in (3.9), we obtain

$$a_0 = 0, \quad a_1 = 0, \quad a_2 = 0.$$

Thus the map (3.7) after restriction to the center manifold is given by

$$F_1 : u_{n+1} = \left(-1 + \frac{\mu_1}{b+1} \right) u + \frac{-1}{b+1}(-\mu_1 + 2b\mu_1 - 3b + b^2 + 1)u^2 + O((|u| + |\mu_1|)^4). \quad (3.10)$$

Since

$$\begin{aligned} \alpha_1 &= \left(2 \frac{\partial^2 F_1}{\partial \mu_1 \partial u} + \frac{\partial F_1}{\partial \mu_1} \frac{\partial^2 F_1}{\partial u^2} \right)_{(0,0)} = \frac{2}{b+1} \neq 0, \\ \alpha_2 &= \left(\frac{1}{2} \left(\frac{\partial^2 F_1}{\partial u^2} \right)^2 + \frac{1}{3} \left(\frac{\partial^3 F_1}{\partial u^3} \right) \right)_{(0,0)} = \frac{2(-3b + b^2 + 1)^2}{(b+1)^2} \neq 0. \end{aligned}$$

Thus, system (1.1) undergoes a subcritical flip bifurcation at $fix_1(0, 0)$. \square

3.2. Bifurcation of fix_2

The Jacobian matrix at $fix_2 = (\frac{a+b-1}{(a+b)^2}, \frac{a+b-1}{(a+b)^2})$, reads

$$J(fix_1) = \begin{pmatrix} a - 2a(ax^* + by^*) & b - 2b(ax^* + by^*) \\ 1 & 0 \end{pmatrix},$$

with $(x^*, y^*) = (\frac{a+b-1}{(a+b)^2}, \frac{a+b-1}{(a+b)^2})$. The characteristic equation

$$F(\lambda) = \lambda^2 + B\lambda + A = 0, \quad (3.11)$$

where $B = \frac{a(a+b-2)}{a+b}$ and $A = \frac{b(a+b-2)}{a+b}$, has two eigenvalues $\lambda_{1,2} = \frac{-B \pm \sqrt{b^2 - 4A}}{2}$.

In this section, the occurrence of both flip and Neimark–Sacker bifurcations in system (1.1) is investigated at the interior fixed point fix_2 where a is taken as the bifurcation parameter. First of all, the occurrence of flip bifurcation of (1.1) is discussed.

Let

$$FB_1 = \left\{ (a, b) : a = \frac{3}{2} + \sqrt{\left(b - \frac{1}{2}\right)^2 + 2}, a \neq 2 - b, \frac{-b(b-4)}{b-2}, b \neq 0, 2 \right\},$$

or

$$FB_2 = \left\{ (a, b) : a = \frac{3}{2} - \sqrt{\left(b - \frac{1}{2}\right)^2 + 2}, a \neq 2 - b, \frac{-b(b-4)}{b-2}, b \neq 0, 2 \right\}.$$

The fixed point fix_2 may admit a flip bifurcation when parameters vary in a small neighborhood of FB_1 or FB_2 . Let

$$NS = \left\{ (a, b) : a = \frac{-b(3-b)}{1-b}, a^2 < \frac{4(a+b)}{a+b-2}, a+b \neq 2, b \neq 1 \right\}.$$

The fixed point fix_2 may undergo a Neimark–Sacker bifurcation when parameters vary in a small neighborhood of NS .

We first discuss the flip bifurcation of (1.1) at $\text{fix}_2(x^*, y^*)$ when parameters vary in a small neighborhood of FB_1 . The same procedure can be applied to FB_2 . Now consider the parameters taken from FB_1 , system (1.1) is described by

$$\begin{cases} x \rightarrow (ax+by)(1-ax-by), \\ y \rightarrow x. \end{cases} \quad (3.12)$$

The map (3.12) has a unique interior fixed point $\text{fix}_2(x^*, y^*)$, whose eigenvalues are $\lambda_1 = -1$, $\lambda_2 = \frac{-a^2-ab+2a}{2(a+b)} + \frac{\sqrt{a^2(a^2+4a+a)+4b^2(-b+2)+ab(ab-8a+2a^2-8b+8)}}{2(a+b)}$ with $|\lambda_2| \neq 1$. Since $(a, b) \in FB_1$, choosing a^* as a bifurcation parameter, we consider a perturbation of (3.12) given by:

$$\begin{cases} x \rightarrow ((a+a^*)x+by)(1-(a+a^*)x-by), \\ y \rightarrow x, \end{cases} \quad (3.13)$$

where $|a^*| \ll 1$ is a small perturbation parameter.

Let $u = x - x^*$, $v = y - y^*$. Transform $\text{fix}_2(x^*, y^*)$ of (3.13) into the origin, we obtain

$$\begin{cases} u \rightarrow a_1u + a_2v + a_{11}u^2 + a_{12}uv + a_{22}v^2 + a_{13}ua^* + a_{23}va^* + a_{123}uva^* + O(|u| + |v| + |a^*|)^4, \\ v \rightarrow b_1u, \end{cases} \quad (3.14)$$

where

$$\begin{cases} a_1 = a - 2a^2x^* - 2aby^*, & a_2 = b - 2a^2y^* - 2abx^*, \\ a_{11} = -a^2, & a_{22} = -b^2, \\ a_{12} = -2ab, & a_{13} = 1 - 4ax^* - 2by^*, \\ a_{23} = -2bx^*, & a_{123} = -2b, \\ b_1 = 1. \end{cases} \quad (3.15)$$

Constructing an invertible matrix

$$T = \begin{pmatrix} a_2 & a_2 \\ -1 - a_1 & \lambda_2 - a_1 \end{pmatrix},$$

and using the translation

$$\begin{pmatrix} u \\ v \end{pmatrix} = T \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix},$$

we obtain that

$$\begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} + \begin{pmatrix} f_1(\tilde{x}, \tilde{y}, a^*) \\ f_2(\tilde{x}, \tilde{y}, a^*) \end{pmatrix}, \quad (3.16)$$

where

$$\begin{aligned} f_1(\tilde{x}, \tilde{y}, a^*) &= \frac{\lambda_2 - a_1}{a_2(1 + \lambda_2)} (a_{11}u^2 + a_{12}uv + a_{22}v^2 + a_{13}ua^* + a_{23}va^* + a_{123}uva^*) + O(|u| + |v| + |a^*|)^4, \\ f_2(\tilde{x}, \tilde{y}, a^*) &= \frac{1 + a_1}{a_2(1 + \lambda_2)} (a_{11}u^2 + a_{12}uv + a_{22}v^2 + a_{13}ua^* + a_{23}va^* + a_{123}uva^*) + O(|u| + |v| + |a^*|)^4, \end{aligned}$$

and

$$\begin{aligned} u &= a_2(\tilde{x} + \tilde{y}), & v &= -(1 + a_1)\tilde{x} + (\lambda_2 - a_1)\tilde{y}, \\ u^2 &= a_2^2(\tilde{x}^2 + \tilde{x}\tilde{y} + \tilde{y}^2), \\ uv &= a_2(-(1 + a_1)\tilde{x}^2 + (\lambda_2 - 2a_1 - 1)\tilde{x}\tilde{y} + a_2(\lambda_2 - a_1)\tilde{y}^2), \\ v^2 &= (1 + a_1)^2\tilde{x}^2 + (\lambda_2 - a_1)^2\tilde{y}^2 - 2(1 + a_1)(\lambda_2 - a_1)\tilde{x}\tilde{y}. \end{aligned}$$

There exists a center manifold $W_c(0, 0, 0)$ of (3.16) at $\text{fix}_1 = (0, 0)$ in a small neighborhood of a^* in the following form

$$W_c(0, 0, 0) = \{(\tilde{x}, \tilde{y}, a^*) \in R^3, \tilde{y} = h(\tilde{x}, a^*), h(0, 0) = 0, Dh(0, 0) = 0\},$$

for \tilde{x} and a^* sufficiently small. Suppose there exists a center manifold in given by

$$h(\tilde{x}, a^*) = m_0\tilde{x}^2 + m_1\tilde{x}a^* + m_2a^{*2} + O((|\tilde{x}| + |a^*|)^3). \quad (3.17)$$

The following relation must be satisfied by the center manifold

$$h(-\tilde{x} + f_1(\tilde{x}, h(\tilde{x}, a^*), a^*), a^*) = \lambda_2 h(\tilde{x}, a^*) + f_2(\tilde{x}, h(\tilde{x}, a^*), a^*). \quad (3.18)$$

Substituting (3.17) into (3.18), then equating like powers' coefficients in (3.18), we obtain

$$\begin{aligned} m_0 &= \frac{a_{11}a_2(1 + a_1)}{1 - \lambda_2^2}, \\ m_1 &= \frac{-a_{13}(1 + a_1)}{(1 + \lambda_2)^2}, \\ m_2 &= 0. \end{aligned}$$

Thus, system (3.16) after restriction to the center manifold $W_c(0, 0, 0)$ is given by:

$$F : \tilde{x} \rightarrow -\tilde{x} + A\tilde{x}^2 + B\tilde{x}^3 + C\tilde{x}^4 + D\tilde{x}a^* + E\tilde{x}^2a^* + F\tilde{x}^3a^* + G\tilde{x}a^{*2} + H\tilde{x}^2a^{*2} + I\tilde{x}^3a^{*2} + O((|\tilde{x}| + |a^*|)^6), \quad (3.19)$$

where

$$\begin{aligned} A &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(a_{11}a_2^2 - a_{12}a_2(1 + a_1) + a_{22}(1 + a_1)^2), \\ B &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(2a_{11}a_2^2m_0 - a_{12}a_2(1 + a_1)m_0), \\ C &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(a_{11}a_2^2m_0^2 + a_{12}a_2m_0^2 + a_{22}(\lambda_2 - a_1)^2m_0^2), \\ D &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(a_{13}a_2 - a_{23}(1 + a_1)m_1), \\ E &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(2a_{11}a_2^2 - a_{12}a_2(1 + a_1)m_1 + a_{23}(\lambda_2 - a_1)m_0), \\ F &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(2a_{11}a_2(\lambda_2 - a_1)m_0m_1 + a_{123}a_2m_0(\lambda_2 - a_1)), \\ G &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(a_{13}a_2m_1 + a_{23}(\lambda_2 - a_1)m_1), \\ H &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(a_{11}a_2^2m_1^2 + a_{12}a_2m_1^2(\lambda_2 - a_1) + a_{123}a_2m_1(1 + a_1)), \\ I &= \frac{\lambda_2 - a_1}{a_2(\lambda_2 + 1)}(2a_{11}a_2(a_{12}a_2)(\lambda_2 - a_1)m_0m_1 + a_{123}a_2m_0m_1). \end{aligned}$$

The system (3.19) admits a flip bifurcation if the quantities α_1 and α_2 do not equal zero, where

$$\alpha_1 = \left(2 \frac{\partial^2 F}{\partial a^* \partial \tilde{x}} + \frac{\partial F}{\partial a^*} \frac{\partial F}{\partial \tilde{x}}\right)_{(0,0)} = 2D \neq 0,$$

$$\alpha_2 = \left(\frac{1}{2} \left(\frac{\partial^2 F}{\partial \tilde{x}^2}\right)^2 + \frac{1}{3} \left(\frac{\partial^3 F}{\partial \tilde{x}^3}\right)\right)_{(0,0)} = 2(A^2 + B).$$

This completes the proof.

Next, we discuss the occurrence Neimark–Sacker bifurcation of $\text{fix}_2(x^*, y^*)$ if parameters (a_c, b) vary in a small neighborhood of NS. Consider the parameters (a, b) are taken arbitrarily from NS, the system (1.1) is described by

$$\begin{cases} x \rightarrow (a_c x + b y)(1 - a_c x - b y), \\ y \rightarrow x. \end{cases} \quad (3.20)$$

System (3.20) has a unique interior fixed point $\text{fix}_2(x^*, y^*)$. Since parameters $(a_c, b) \in \text{NS}$, then $a_c = -\frac{b^2 - 3b}{1-b}$. Choosing a^* as a bifurcation parameter, we consider a small perturbation of the system (3.20) in the following form:

$$\begin{cases} x \rightarrow ((a_c + \bar{a}^*)x + b y)(1 - (a_c + \bar{a}^*)x - b y), \\ y \rightarrow x \end{cases} \quad (3.21)$$

where $\bar{a}^* \ll 1$, is a small perturbation parameter.

Let $u = x - x^*$, $v = y - y^*$. Transforming $\text{fix}_2(x^*, y^*)$ of (3.21) into the origin, we obtain

$$\begin{cases} u \rightarrow a_1 u + a_2 v + a_{11} u^2 + a_{12} u v + a_{22} v^2 + O((|u| + |v| + |\bar{a}^*|)^4), \\ v \rightarrow b_1 u, \end{cases} \quad (3.22)$$

where $a_1, a_2, a_{11}, a_{12}, a_{22}$ and b_1 are given in (3.14) by substituting a for $a_c + \bar{a}^*$.

The characteristic equation associated to system (3.22) at $(u, v) = (0, 0)$ can be written as

$$\lambda^2 + B(\bar{a}^*)\lambda + A(\bar{a}^*) = 0,$$

where

$$B(\bar{a}^*) = \frac{(a_c + \bar{a}^*)(a_c + \bar{a}^* - 2)}{a_c + \bar{a}^* + b},$$

$$A(\bar{a}^*) = \frac{b(a_c + \bar{a}^* + b - 2)}{a_c + \bar{a}^* + b}.$$

Since parameters $(a_c, b) \in \text{NS}$, the eigenvalues of the origin are a pair of complex conjugate numbers λ and $\bar{\lambda}$ with $|\lambda| = 1$ and $|\bar{\lambda}| = 1$ by Lemma 2, where

$$\lambda, \bar{\lambda} = -\frac{B(\bar{a}^*)}{2} \pm \frac{i}{2}\sqrt{4B(\bar{a}^*) - A^2(\bar{a}^*)},$$

and so

$$|\lambda|_{\bar{a}^*=0} = \sqrt{A(0)} = 1, \quad l = \frac{d|\lambda|}{d\bar{a}^*}|_{\bar{a}^*=0} = \frac{8b^2}{(1-b)^2} \neq 0.$$

In addition, it is required that when $\bar{a}^* = 0$, $\lambda^m, \bar{\lambda}^m \neq 1 (m = 1, 2, 3, 4)$, which is equivalent to $B(0) \neq -2, 0, 1, 2$. Note that $(a_2, b) \in \text{HB}$. Thus, $B(0) \neq -2, 2$. We only need to require that $p(0) \neq 0, 1$, which leads to

$$3b^2 \neq b, b+1. \quad (3.23)$$

Therefore, the eigenvalues $\lambda, \bar{\lambda}$ of $\text{fix}_1 = (0, 0)$ of the system (3.22) do not lie in the intersection of the unit circle with the coordinate axes when $\bar{a}^* = 0$ and the condition (3.23) holds.

Now, we discuss the normal form of (3.22) at $\bar{a}^* = 0$.

$$\text{Let } \bar{a}^* = 0, \sigma = \frac{-a(a+b-2)}{a+b}, \omega = \sqrt{\frac{4b(a+b)(a+b-2)-a^2(a+b-2)}{(a+b)^2}}.$$

Constructing an invertible matrix

$$T = \begin{pmatrix} a_2 & 0 \\ \sigma - a_1 & -\omega \end{pmatrix},$$

and using the translation

$$\begin{pmatrix} u \\ v \end{pmatrix} = T \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix},$$

the system (3.22) becomes

$$\begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} \rightarrow \begin{pmatrix} \sigma & -\omega \\ \omega & \sigma \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} + \begin{pmatrix} \bar{f}_1(\tilde{x}, \tilde{y}) \\ \bar{f}_2(\tilde{x}, \tilde{y}) \end{pmatrix}, \quad (3.24)$$

where

$$\bar{f}_1(\tilde{x}, \tilde{y}) = \frac{a_{11}}{a_2}u^2 + \frac{a_{12}}{a_2}uv + \frac{a_{22}}{a_2}v^2 + O((|\tilde{x}| + |\tilde{y}|)^3),$$

$$\bar{f}_2(\tilde{x}, \tilde{y}) = \frac{\sigma - a_1}{a_2\omega}(a_{11}u^2 + a_{12}uv + a_{22}v^2) + O((|\tilde{x}| + |\tilde{y}|)^3),$$

and

$$\begin{aligned} u &= a_2 \tilde{x}, v = (\sigma - a_1) \tilde{x} - \omega \tilde{y}, \\ uv &= a_2(\mu - a_1) \tilde{x}^2 - a_2 \omega \tilde{x} \tilde{y}, \\ u^2 &= a_2^2 \tilde{x}^2, \quad v^2 = (\sigma - a_1)^2 \tilde{x}^2 + \omega^2 \tilde{y}^2 - 2(\sigma - a_1) \omega \tilde{x} \tilde{y}. \end{aligned}$$

Therefore,

$$\begin{aligned} \bar{f}_{1\tilde{x}\tilde{x}} &= 2a_{11}a_2 + 2\frac{a_{22}}{a_2}(1+a_1)^2, \\ \bar{f}_{1\tilde{x}\tilde{y}} &= \frac{a_{12}}{a_2}(-2(\sigma - a_1)\omega) + \frac{a_{22}}{a_2}(-2(1+a_1)(\lambda_2 - a_1)), \\ \bar{f}_{1\tilde{y}\tilde{y}} &= 2\frac{a_{12}}{a_2}\omega^2 + \frac{a_{22}}{a_2}(\lambda_2 - a_1), \\ \bar{f}_{1\tilde{x}\tilde{x}\tilde{y}} &= \bar{f}_{1\tilde{x}\tilde{y}\tilde{y}} = \bar{f}_{1\tilde{y}\tilde{y}\tilde{y}} = \bar{f}_{1\tilde{x}\tilde{x}\tilde{x}} = 0, \\ \bar{f}_{2\tilde{x}\tilde{x}} &= \frac{\sigma - a_1}{a_2\omega}(2a_{11}a_2^2 + 2a_{12}a_2)(\mu - a_1) + 2a_{22}(\sigma - a_1)^2, \\ \bar{f}_{2\tilde{x}\tilde{y}} &= \frac{\sigma - a_1}{a_2\omega}(-a_{12}a_2\omega - 2a_{22}(\sigma - a_1)\omega), \\ \bar{f}_{2\tilde{y}\tilde{y}} &= 2\frac{\sigma - a_1}{a_2\omega}(a_{22}\omega^2), \\ \bar{f}_{2\tilde{x}\tilde{x}\tilde{y}} &= \bar{f}_{2\tilde{x}\tilde{y}\tilde{y}} = \bar{f}_{2\tilde{y}\tilde{y}\tilde{y}} = \bar{f}_{2\tilde{x}\tilde{x}\tilde{x}} = 0, \end{aligned}$$

at the origin.

The system (3.24) may undergo a Neimark–Sacker bifurcation if the following quantity does not equal zero:

$$L = \left[-Re\left(\frac{(1-2\lambda)\bar{\lambda}^2}{1-\lambda}L_{11}L_{12}\right) - \frac{1}{2}|L_{11}|^2 - |L_{21}|^2 + Re(\bar{\lambda}L_{22}) \right]_{\bar{a}^*=0},$$

where

$$\begin{aligned} L_{11} &= \frac{1}{4}((\bar{f}_{1\tilde{x}\tilde{x}} + \bar{f}_{1\tilde{y}\tilde{y}}) + i(\bar{f}_{2\tilde{x}\tilde{x}} + \bar{f}_{2\tilde{y}\tilde{y}})), \\ L_{12} &= \frac{1}{8}((\bar{f}_{1\tilde{x}\tilde{x}} - \bar{f}_{1\tilde{y}\tilde{y}} + 2\bar{f}_{2\tilde{x}\tilde{y}}) + i(\bar{f}_{2\tilde{x}\tilde{x}} - \bar{f}_{2\tilde{y}\tilde{y}} - 2\bar{f}_{1\tilde{x}\tilde{y}})), \\ L_{21} &= \frac{1}{8}((\bar{f}_{1\tilde{x}\tilde{x}} - \bar{f}_{1\tilde{y}\tilde{y}} - 2\bar{f}_{2\tilde{x}\tilde{y}}) + i(\bar{f}_{2\tilde{x}\tilde{x}} - \bar{f}_{2\tilde{y}\tilde{y}} + 2\bar{f}_{1\tilde{x}\tilde{y}})), \\ L_{22} &= \frac{1}{16}((\bar{f}_{1\tilde{x}\tilde{x}\tilde{x}} + \bar{f}_{1\tilde{x}\tilde{y}\tilde{y}} + \bar{f}_{2\tilde{x}\tilde{x}\tilde{y}} + \bar{f}_{2\tilde{y}\tilde{y}\tilde{y}}) + i(\bar{f}_{2\tilde{x}\tilde{x}\tilde{x}} + \bar{f}_{2\tilde{x}\tilde{y}\tilde{y}} - \bar{f}_{1\tilde{x}\tilde{x}\tilde{y}} - \bar{f}_{1\tilde{y}\tilde{y}\tilde{y}})). \end{aligned}$$

According to the preceding analysis we can state the following result based on [60].

Theorem 1. System (1.1) undergoes Neimark–Sacker bifurcation at the fixed point $\text{fix}_2(x^*, y^*)$ under the conditions (3.23) and $L \neq 0$, when a is close to a_2 . Moreover, if $L < 0$ (resp., $L > 0$), then an attracting (resp., repelling) invariant closed curve bifurcates from the fixed point for $a > a_2$ (resp., $a < a_2$).

4. Existence of Marotto's chaos

In this section, we prove that the system (1.1) is chaotic in the sense of Marotto.

Definition 1 ([61]). Let the function $F : R^n \rightarrow R^n$ be differentiable in $B_r(Z)$. The point $Z \in R^n$ is an expanding fixed point of F in $B_r(Z)$, if $F(Z) = Z$ and all eigenvalues of $DF(X)$ exceed 1 in norm for all $X \in B_r(Z)$.

Definition 2 ([61]). Assume that Z is an expanding fixed point of F in $B_r(Z)$ for some $r > 0$. Then Z is said to be a snapback repeller of F if there exists a point $X_0 \in B_r(Z)$ with $X_0 \neq Z$, $F^M(X_0) = Z$ and $DF^M(X_0) \neq 0$ for some positive integer M .

Now we state the theorem due to Marotto [61].

Theorem 2. If f is differentiable and has a snap-back repeller, the system (1.1) is chaotic in the sense of Li–Yorke, and

- (a) there is a positive integer N such that for each integer $p \geq N$, f has a point of period p , and
- (b) there is a “scrambled set” of f , i.e., an uncountable set S containing no periodic points of f such that:

$$(b-1) \quad f(S) \subset S,$$

$$(b-2) \quad \text{for every } X_S; Y_S \in S \text{ with } X_S \neq Y_S,$$

$$\lim_{k \rightarrow +\infty} \sup \|f^k(X_S) - f^k(Y_S)\| > 0,$$

$$(b-3) \quad \text{for every } X_S \in S \text{ and any periodic point } Y_{per} \text{ of } f,$$

$$\lim_{k \rightarrow +\infty} \sup \|f^k(X_S) - f^k(Y_{per})\| > 0;$$

$$(c) \quad \text{there is an uncountable subset } S_0 \text{ of } S \text{ such that for every } X_{S_0}; Y_{S_0} \in S_0:$$

$$\lim_{k \rightarrow +\infty} \sup \|f^k(X_{S_0}) - f^k(Y_{S_0})\| = 0.$$

Firstly, we give the condition that fix_2 is an expanding fixed point of system (1.1) which is given by

$$F(X_n) = \begin{pmatrix} (ax_n + by_n)(1 - ax_n - by_n) \\ x_n \end{pmatrix},$$

where $X_n = (x_n \ y_n)^T$. The eigenvalues corresponding to the fixed point fix_2 are given by

$$\lambda_{1,2} = \frac{-B \pm \sqrt{B^2 - 4A}}{2},$$

where

$$B = \frac{b(a+b-2)}{a+b},$$

$$A = \frac{a(a+b-2)}{a+b}.$$

Let $\lambda_{1,2}$ be a pair of complex eigenvalues with $|\lambda_{1,2}| > 1$, that is

$$\begin{cases} B^2 - 4A < 0, \\ A > 1. \end{cases}$$

Let

$$S_1(x, y) = a^2(1 + 2a(ax + by))^2 + 4b(1 - 2(ax + by)),$$

if $y > 0$, then for

$$a^2(1 + 2a(ax + by))^2 + 4b(1 - 2(ax + by)) < 0,$$

we have

$$-O^* < x < O^*,$$

where

$$O^* = \sqrt{\frac{8ba^4(2by - 1) - 2a^6(2b^2y^2 + 1) + (4ab - 2a^3by)^2}{4a^8}}.$$

Thus, if $x \in D_1 = \{x \mid -O^* < x < O^*\}$ and $y > 0$, then $S_1(x, y) < 0$.

Let

$$S_2(x, y) = -b + 2b(ax + by) - 1,$$

if $y > \frac{1+b-2abx}{2b^2}$, then for

$$-b + 2b(ax + by) - 1 > 0,$$

we have

$$x > \frac{1 + b - 2b^2y}{2ab}.$$

Thus, if $x \in D_2 = \{x \mid x > \frac{1+b-2b^2y}{2ab} \text{ and } y > \frac{1+b-2abx}{2b^2}\}$, then $S_2(x, y) > 0$.

The following Lemma may be stated according to the above analysis

Lemma 4. Let $a, b > 0$, if $x \in D_1 \cap D_2$ and $y > 0$, then $S_1(x, y) < 0$ and $S_2(x, y) > 0$. Moreover, if the fixed point $\text{fix}_2 = z^*(x^*, y^*)$ of map (1.1) satisfies

$$z^*(x^*, y^*) \in U_{z^*} = \{(x, y) | x \in D_1 \cap D_2, y > 0\},$$

then $z^*(x^*, y^*)$ is an expanding fixed point in U_{z^*} .

Now we should find a point $z_1(x_1, y_1) \in U_{z^*}$ such that $z_1 \neq z^*$, $F^N(z_1) = z^*$, $|DF^N(z_1)| \neq 0$, for some positive integer N , where F is Marotto's map (1.1).

Note that

$$\begin{aligned} (ax_1 + by_1)(1 - ax_1 - by_1) &= x_2, \\ x_1 &= y_2. \end{aligned} \tag{4.1}$$

Moreover,

$$\begin{aligned} (ax_2 + by_2)(1 - ax_2 - by_2) &= x^*, \\ x_2 &= y^*. \end{aligned} \tag{4.2}$$

Hence we can map the point $z_1(x_1, y_1)$ to the fixed point $z^*(x^*, y^*)$ by iterating the map F two times if there are solutions for Eqs. (4.1) and (4.2) which will be different from z^* . The solutions different from z^* for Eq. (4.2) satisfy the following equation

$$\begin{aligned} x_2 &= y^*, \\ y_2 &= -a^2y^{*2} - 2aby_2y^* + ay^* - b^2y_2^2 + by_2. \end{aligned} \tag{4.3}$$

Substituting x_2 and y_2 into Eq. (4.1) and solving for x_1, y_1 , we have

$$\begin{aligned} x_1 &= -(ax_1 + by_1)^2(a^2(ax_1 + by_1)^2 - 2abx_1 + a) - b^2x_1^2 + bx_1, \\ y_1 &= \frac{x_1}{b(1 - ax_1 - by_1)} - \frac{ax_1}{b}. \end{aligned} \tag{4.4}$$

By direct calculations we obtain

$$|DF^2(Z_1)| = b(A^* + B^*)(-2aA^*B^* + 2bx - 1)(a^2A^* + a^2B^* - b + ab(A^* + B^*)),$$

where $A^* = ax + by$ and $B^* = ax + by - 1$.

If conditions in Lemma 4 are satisfied, then solutions of Eqs. (4.3) and (4.4) are subject to $z_1(x_1, y_1), z_2(x_2, y_2) \neq z^*(x^*, y^*)$, $z_1(x_1, y_1) \in U_{z^*}$ and $|DF^2(z_1)| \neq 0$, thus z^* is a snap-back repeller in U_{z^*} . Now the following theorem can be stated

Theorem 3. Assume that those conditions in Lemma 4 hold. If

- (1) $a^2(1 + 2a(ax^* + by^*))^2 + 4b(1 - 2(ax^* + by^*)) < 0$ and $-b + 2b(ax^* + by^*) - 1 > 0$,
- (2) Solutions (x_2, y_2) and (x_1, y_1) of Eqs. (4.3) and (4.4) satisfy in addition $(x_1, y_1), (x_2, y_2) \neq (x^*, y^*), (x_1, y_1) \in U_{z^*}$, $(x_1, y_1) \neq (0, 0)$ and $|DF^2(z_1)| \neq 0$, then $z^*(x^*, y^*)$ is a snap-back repeller of map (1.1), and hence map (1.1) is chaotic in the sense of Marotto.

5. Numerical simulations

All the previous analytical findings are substantiated with the help of numerical simulations performed via Matlab. In all numerical simulations we choose a as the bifurcation parameter and the initial condition is taken as $(x_0, y_0) = (0.1, 0.1)$.

1. Fix $b = 0.5$, then a transcritical bifurcation of the fixed point $\text{fix}_1(0, 0)$ occurs at $a = 0.5$ as can be seen in Fig. 2(a) which agrees with Lemma 3. The corresponding maximal Lyapunov exponent is shown in Fig. 2(b). Now fix $b = 2.5$, then a flip bifurcation of the same fixed point occurs at $a = 1.5$ which agrees with Lemma 4 as depicted in Fig. 2(c) and its corresponding maximal Lyapunov exponent is shown in Fig. 2(d). If we choose $b = 2$, then the interior fixed point will be $\text{fix}_2 = (0.204, 0.204)$ and a flip bifurcation will occur at it when $a = 1.5$ as illustrated in Fig. 3(a). The corresponding maximal Lyapunov exponent is shown in Fig. 3(b). Next, if we take $b = 3$, then according to the analysis of the Neimark–Sacker bifurcation, $a_c = 0$ and according to these parameters we obtain $\text{fix}_2 = (0.2222, 0.2222)$, a Neimark–Sacker bifurcation occurs at it and this can be clearly seen in Fig. 3(c). The corresponding maximal Lyapunov exponent is shown in Fig. 3(d).
2. Choose $a = 0.67$ and $b = 2.5$. In this case we have $\text{fix}_2 = (0.2159, 0.2159)$ which is stable as depicted in Fig. 4(a) according to Proposition 2. Now we vary a and fix $b = 0.5$. The fixed point fix_2 loses its stability at $a = 1.78$ as seen in Fig. 4(b), on account of the norm of complex eigenvalues of its corresponding Jacobian matrix equal to 1. Consequently,

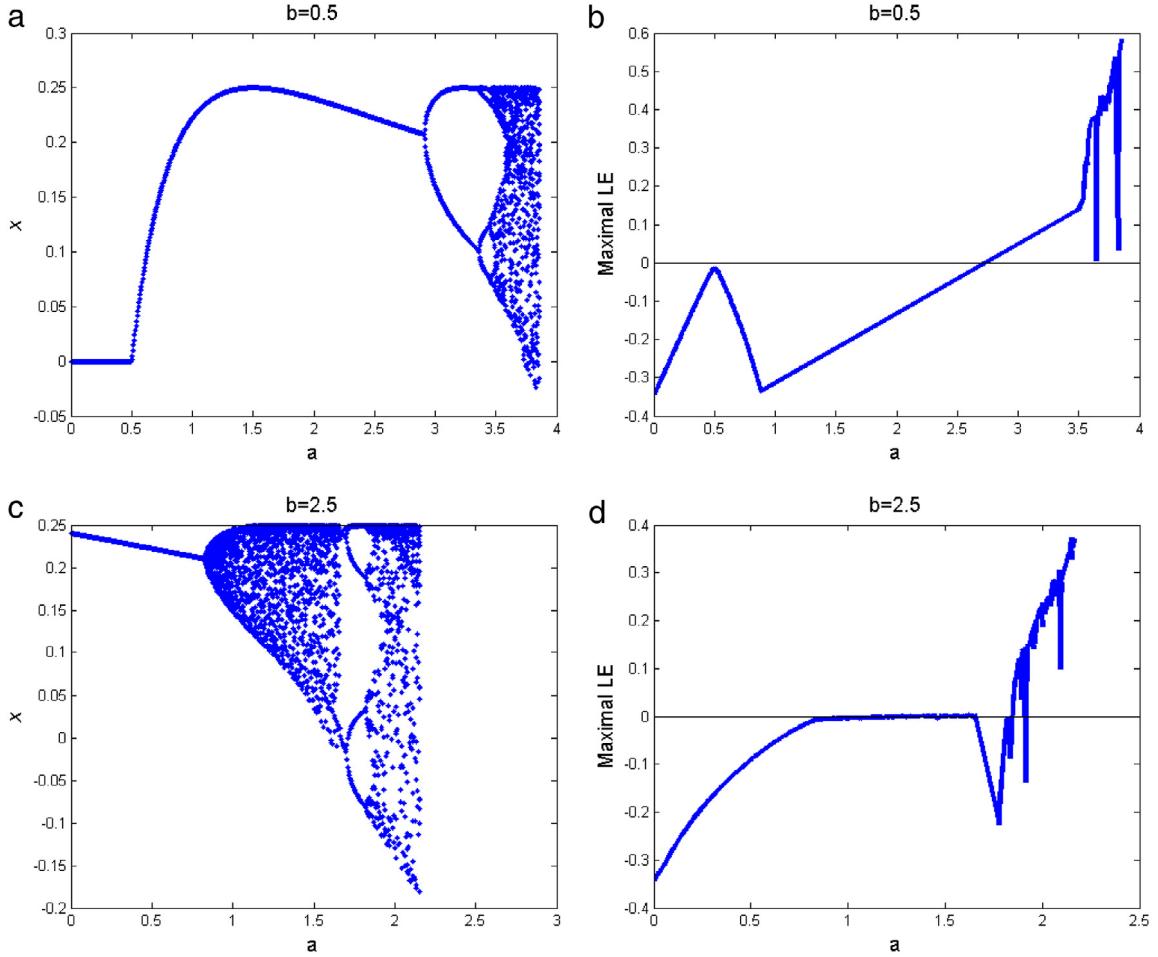


Fig. 2. Bifurcation diagrams and corresponding Maximal Lyapunov exponent of map (1.1) as a function of a with different values of b .

a closed invariant cycle appears at $a = 1.2$ as shown in Fig. 4(c). The breakdown of this cycle is depicted in Fig. 4(d) when $a = 1.35$. Strange attractors are illustrated in Fig. 4(e), (f), (g), (h), for different a and b .

3. For the snap-back repeller we consider the following numerical example:

Take $a = 0.4$ and $b = 3.5$, then map (1.1) has a fixed point $z^* = (x^*, y^*) = (0.7436, 0.7436)$. The eigenvalues of the Jacobian matrix associated to z^* are $\lambda_{1,2} = -0.8527 \pm 0.7295i$ with $|\lambda_{1,2}| > 1$. In this case and by Theorem 3 we have $D_1 = \{x : x > -4.89935 \text{ and } y > 0.09869\}$ and $D_2 = \{-0.0708 < x < 0.0708\}$. Now we can find a point $(x_1, y_1) = (0.23011, 0.1568)$ which satisfies $F^2(x_1, y_1) = (x^*, y^*)$ and $|DF^2(x_1, y_1)| \neq 0$ therefore (x^*, y^*) is a snap-back repeller.

6. Encryption process

In this part of the paper, we apply the Marotto's map for image encryption. A little modification to the encryption scheme presented in [57] will be made which is summed up in replacing the Hénon map with the Marotto's map (1.1) with $a = 0.8$ and $b = 3$. Now the map (1.1) has the following form

$$\begin{aligned} x_{n+1} &= (0.8x_n + 3y_n)(1 - 0.8x_n - 3y_n), \\ y_{n+1} &= x_n. \end{aligned} \quad (6.1)$$

The encryption process is made up of two main steps. In the first step, the Marotto's map is used to implement the positions of pixel permutation. In the second step, a combination of a spatiotemporal chaos and compound chaos is used as value shuffling. The spatiotemporal chaotic map adopted here in the one-way coupled map lattice (OCML) given in the

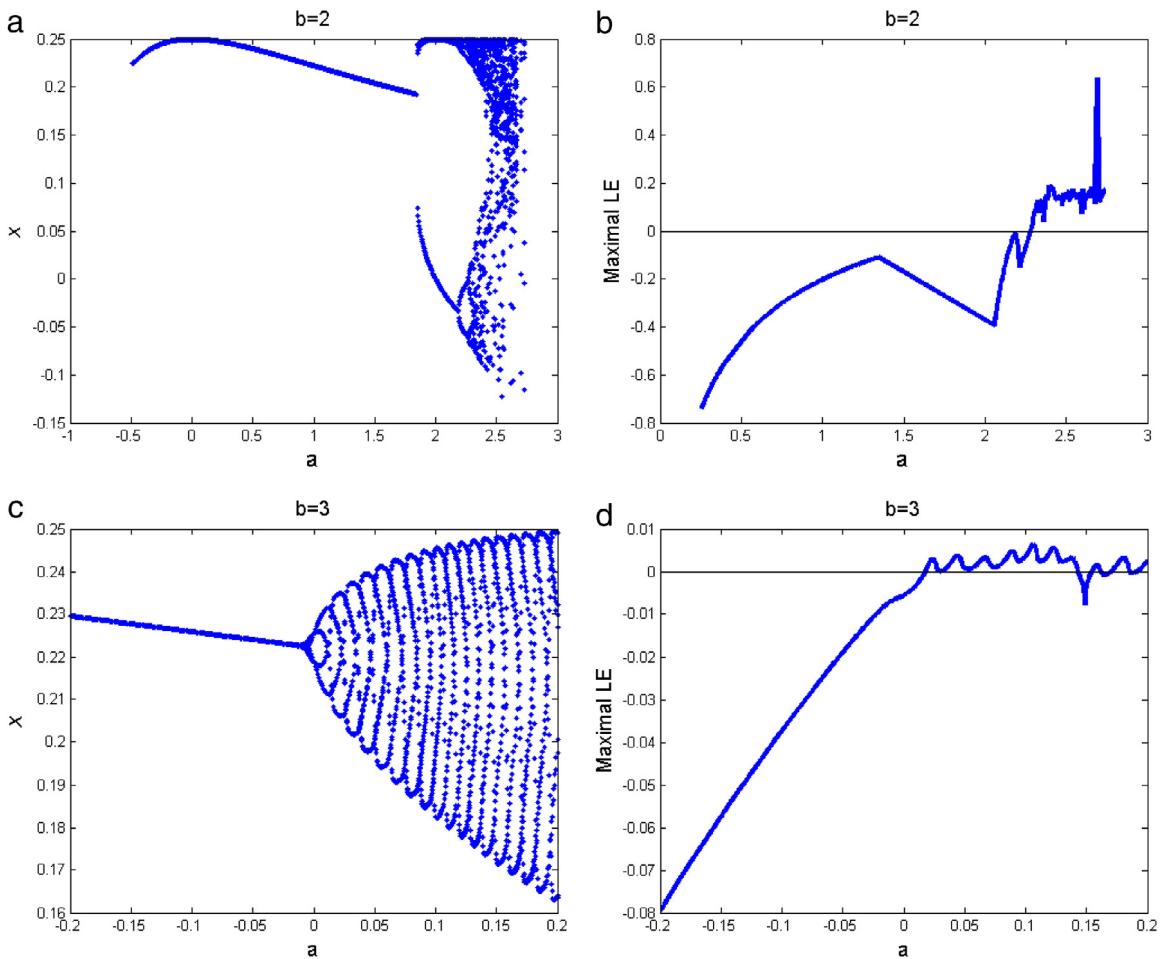


Fig. 3. Bifurcation diagrams and corresponding Maximal Lyapunov exponent of map (1.1) as a function of a with different values of b (Cont.).

form

$$x_{n+1}^i = (1 - \varepsilon)f(x_n^i) + \delta f(x_n^{i-1}),$$

where $i = 0, \dots, N - 1$ is the lattice site index; $n = 0, 1, 2, \dots$ stands for time; $\varepsilon \in (0, 1)$ is the coupling coefficient; f is the Riccati map given by

$$x_{n+1} = 1 - \rho x_n^2, \quad (6.2)$$

with $\rho \in [1.40115, 2]$.

To derive the OCML we use the combination of Logistic map given by

$$x_{n+1} = \mu x_n(1 - x_n), \quad (6.3)$$

where $\mu \in (3.57, 4]$ and Chebyshev map which is given as follows

$$x_{n+1} = \cos(k \cos^{-1} x_n), \quad (6.4)$$

where $k \geq 2$. The initial conditions for the lattices x_0^i , $i = 1, 2, \dots, N$ are those values generated from the chaotic sequence of the Logistic map, while the sequence derived from the Chebyshev map is used for the 0th lattice. Figs. 5 and 6 show the chaotic sequence generated from the Marotto's map and the generation of a matrix W resulted from the combination of the Logistic map and Chebyshev map.

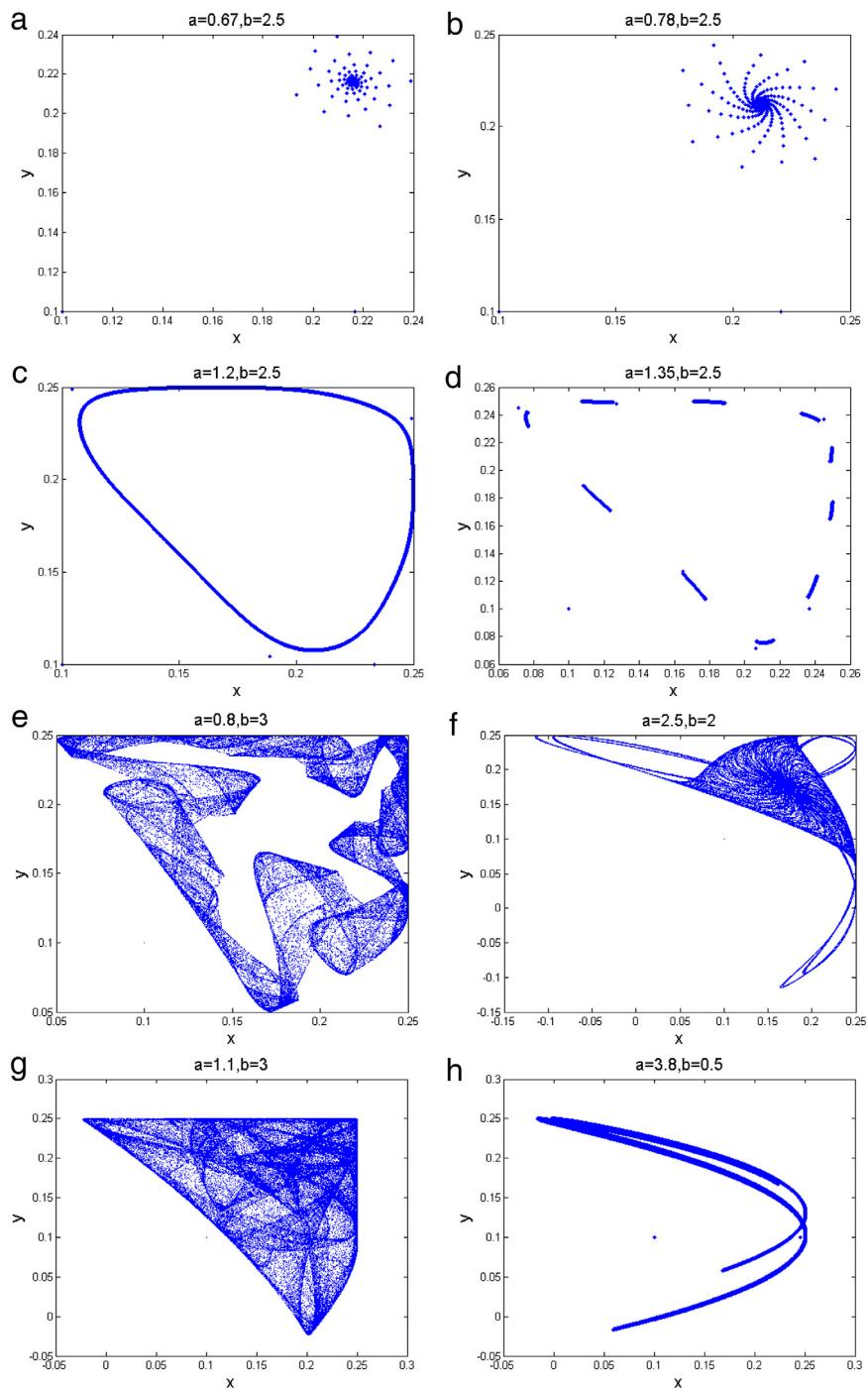
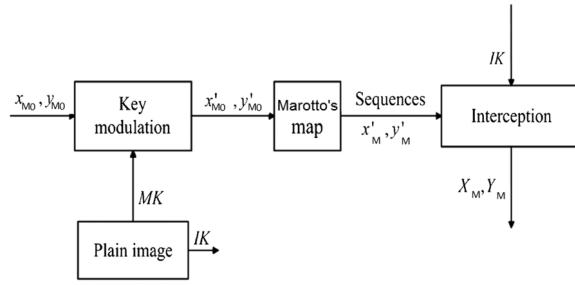
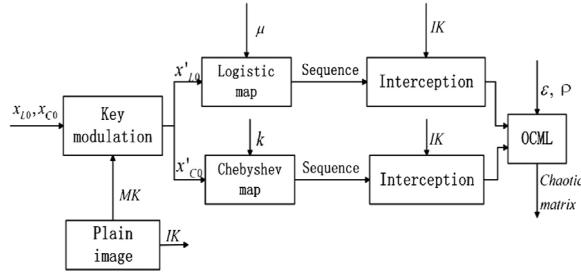


Fig. 4. Phase portraits of map (1.1) for different a and b .

The steps of the encryption process can be summarized as follows:

1. Read the plain image of any size, say $A = M \times N$. The pixel value at the i th row and j th column is A_{ij} , with $1 \leq i \leq M$, and $1 \leq j \leq N$.
2. Put secret keys for the cryptosystem. That is, x_{M0}, y_{M0} for the Marotto's map (6.1), ρ in (6.2), μ and x_{L0} in (6.3), k and x_{C0} in (6.4), and an additional key $K > 10\,001$.

**Fig. 5.** Chaotic sequence generated from the Marotto's map.**Fig. 6.** The chaotic matrix W .

3. Depending on the plain image, a generation of two subkeys to enhance the security of the cryptosystem is described as follows:

- a. An interception key IK generated from the plain image

$$IK = \left(\sum_{i=1}^M \sum_{j=1}^N A(i, j) \right) modK, \quad (6.5)$$

- b. A modulation key also generated from the plain image

$$MK = \frac{IK}{K}. \quad (6.6)$$

4. Modulate x_{M0}, y_{M0}, x_{L0} , and x_{C0} to get new initial conditions as follows

$$x'_{M0} = x_{M0} \times MK. \quad (6.7)$$

$$y'_{M0} = y_{M0} \times MK. \quad (6.8)$$

$$x'_{L0} = x_{L0} \times MK. \quad (6.9)$$

$$x'_{C0} = x_{C0} \times MK. \quad (6.10)$$

5. Perform permutation of pixel positions by iterating the Marotto's map $\max\{M, N\} + IK$ times in order to obtain two chaotic sequences x'_{M0}, y'_{M0} with elements given by

$$X_M = x'_M(IK + a - 1), \quad (6.11)$$

$$Y_M = y'_M(IK + b - 1). \quad (6.12)$$

Then, by the mean of the index function $sort(\cdot)$, generate two chaotic index sequences $index1$ and $index2$, that is

$$index1 = sort|X_M|, \quad (6.13)$$

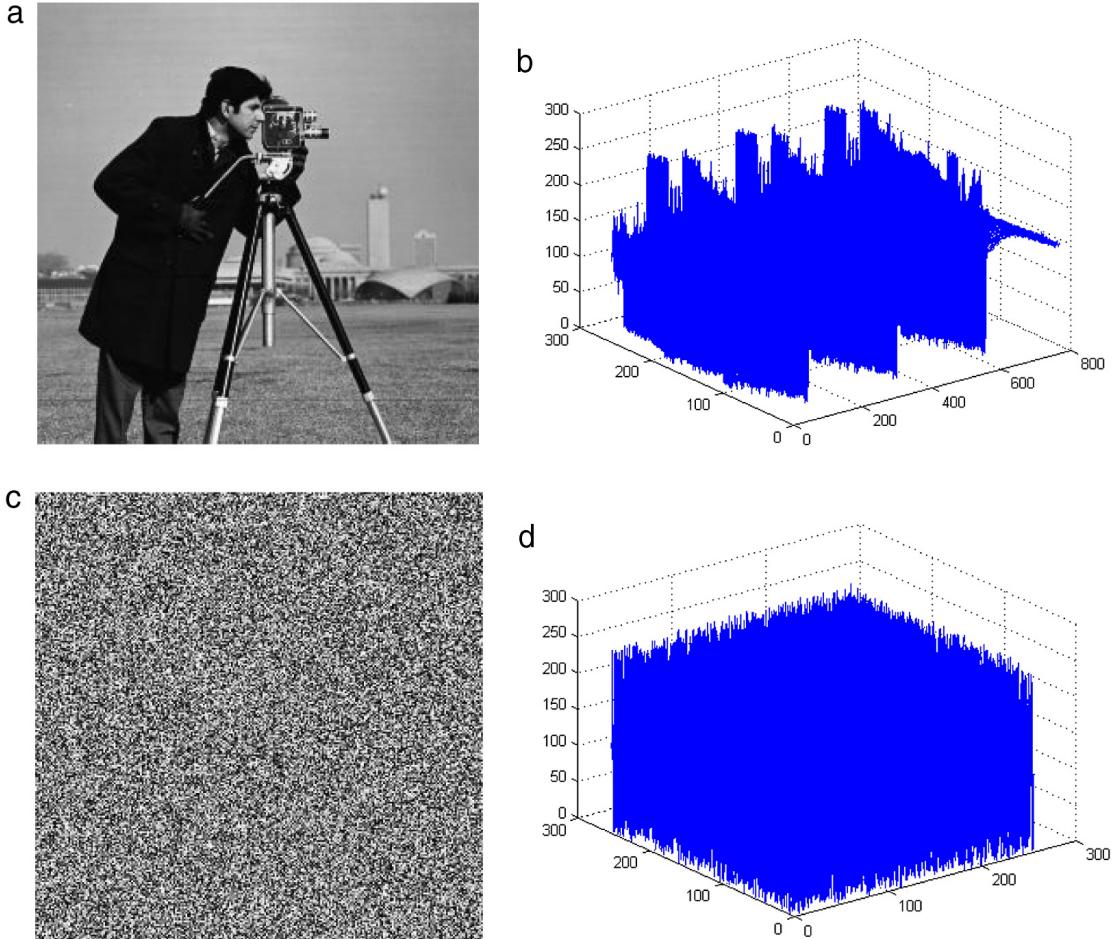


Fig. 7. Spatial characteristic analysis of cameraman image: (a) plain, (b) spatial, (c) ciphered, (d) spatial ciphered.

$$\text{index}2 = \text{sort}|\mathbf{Y}_M|, \quad (6.14)$$

where $|\cdot|$ is the absolute value and the function $\text{sort}(x)$ is used to sort the element of the vector x in ascending order and then returns an index sequence. The permuted image A_1 is obtained by

$$A_1(p, q) = A(\text{index}1(p), \text{index}2(q)). \quad (6.15)$$

6. Shuffle the pixel values as follows:

- a. Iterate the Logistic map $IK + N - 1$ times and the Chebyshev map $IK + M - 1$ times and discard the previous IK values of the two obtained sequences. Then we obtain two chaotic driving sequences d_{Lq} and d_{Cp} from the Logistic and Chebyshev maps respectively, with $1 \leq p \leq M$ and $1 \leq q \leq N$.
- b. Build a chaotic matrix W through the OCML. Let d_C fill the 0 th lattice of the spatiotemporal chaotic system which consists of $N + 1$ lattices. Each value of the sequence d_L is assumed to be an initial value for the first to the N th lattice. By iterating the OCML $M - 1$ times, we get the matrix W which is given in the form

$$W(i, j) = (\text{round}(10^{14}W(i, j))) \bmod 256, \quad (6.16)$$

where $1 \leq i \leq M$ and $1 \leq j \leq N$.

- c. Finally, the shuffled image A_2 is obtained by

$$A_2 = A_1 \oplus W, \quad (6.17)$$

where \oplus is the exclusive OR operation bit-by-bit.

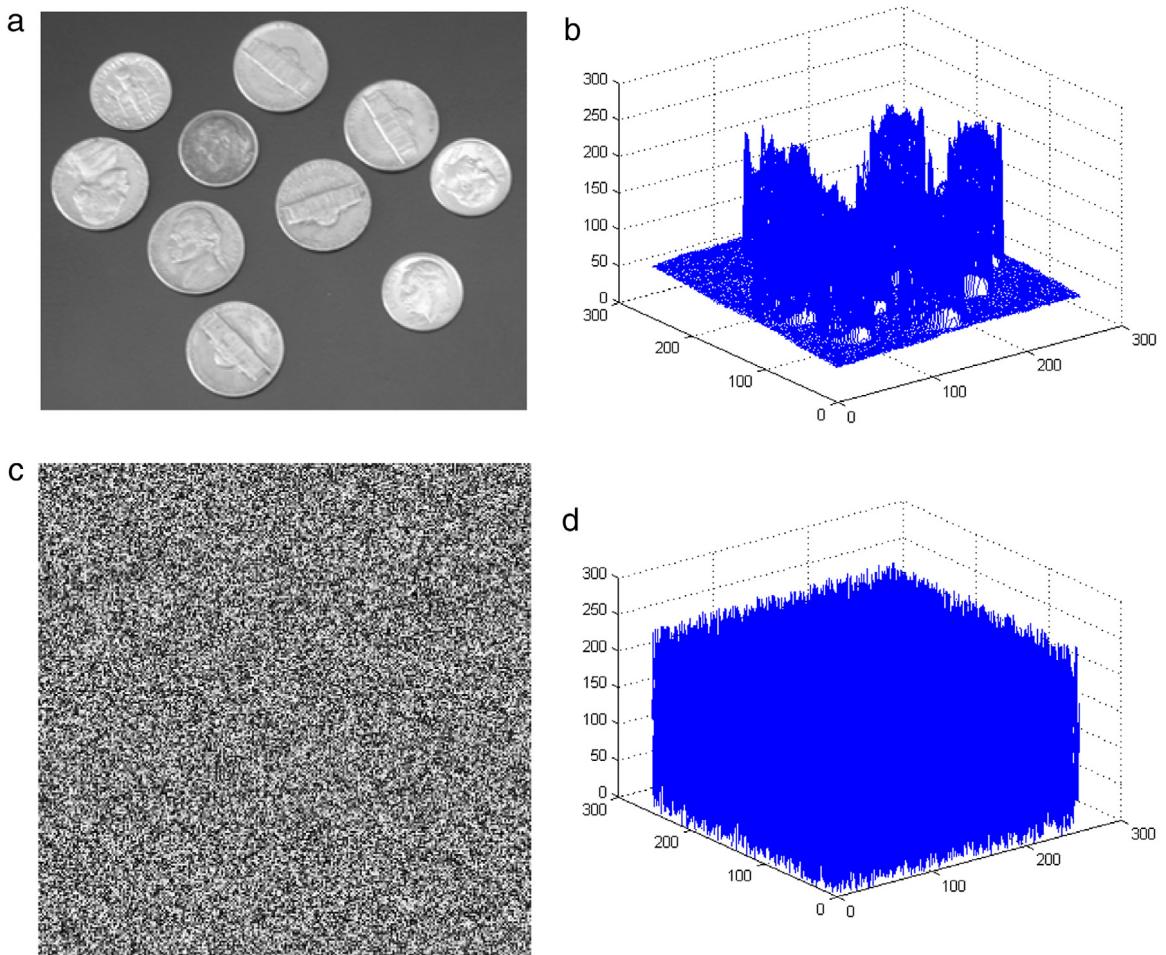


Fig. 8. Spatial characteristic analysis of coins image: (a) plain, (b) spatial, (c) ciphered, (d) spatial ciphered.

6.1. Decryption process

The decryption process is a simple inverse process of the implemented encryption method which is done by reconstructing gray levels of the original image from the encrypted image.

6.2. Simulation results

For an image encryption method to be effective, it should withstand against all types of known attacks. In this section, we test several gray scale images of sizes 256×256 . The initial secret keys are $x_{M0} = 0.1$, $y_{M0} = 0.1$, $\rho = 2$, $\mu = 4$, $x_{L0} = 0.1$, $k = 5$, $K = 10\,001$. Each plain image generates a corresponding interception and modulation keys. In Fig. 7(a), the cameraman image is shown, its spatial image is shown in 7(b), the ciphered image of cameraman is shown in 7(c), and the spatial image of the ciphered cameraman image is shown in 7(d). The same results are obtained for the following images: coins, eight, and pyramids which are shown in Fig. 8, 9, and 10, respectively.

As a spatial characteristic of a spatial image, both X-axis and Y-axis denote the two-dimensional position of a pixel of the image, while the Z-axis denotes the gray scale value of a pixel. Thus, an encrypted image results from a spatiotemporal chaotic system is permuted and shuffled in multiple directions of a space. As a result, it is hard for any attackers to obtain information of the plaintext image via statistical analysis. For key sensitivity analysis, key space, plaintext sensitivity and differential attack analysis, please see [57].

As a matter of fact, the difference between implementing the Hénon map and the Marotto's map in the presented encryption method lies on the richer chaotic dynamics of the later than the first and this is considered as an important feature for cryptography based on chaotic maps since it increases security against attacks.

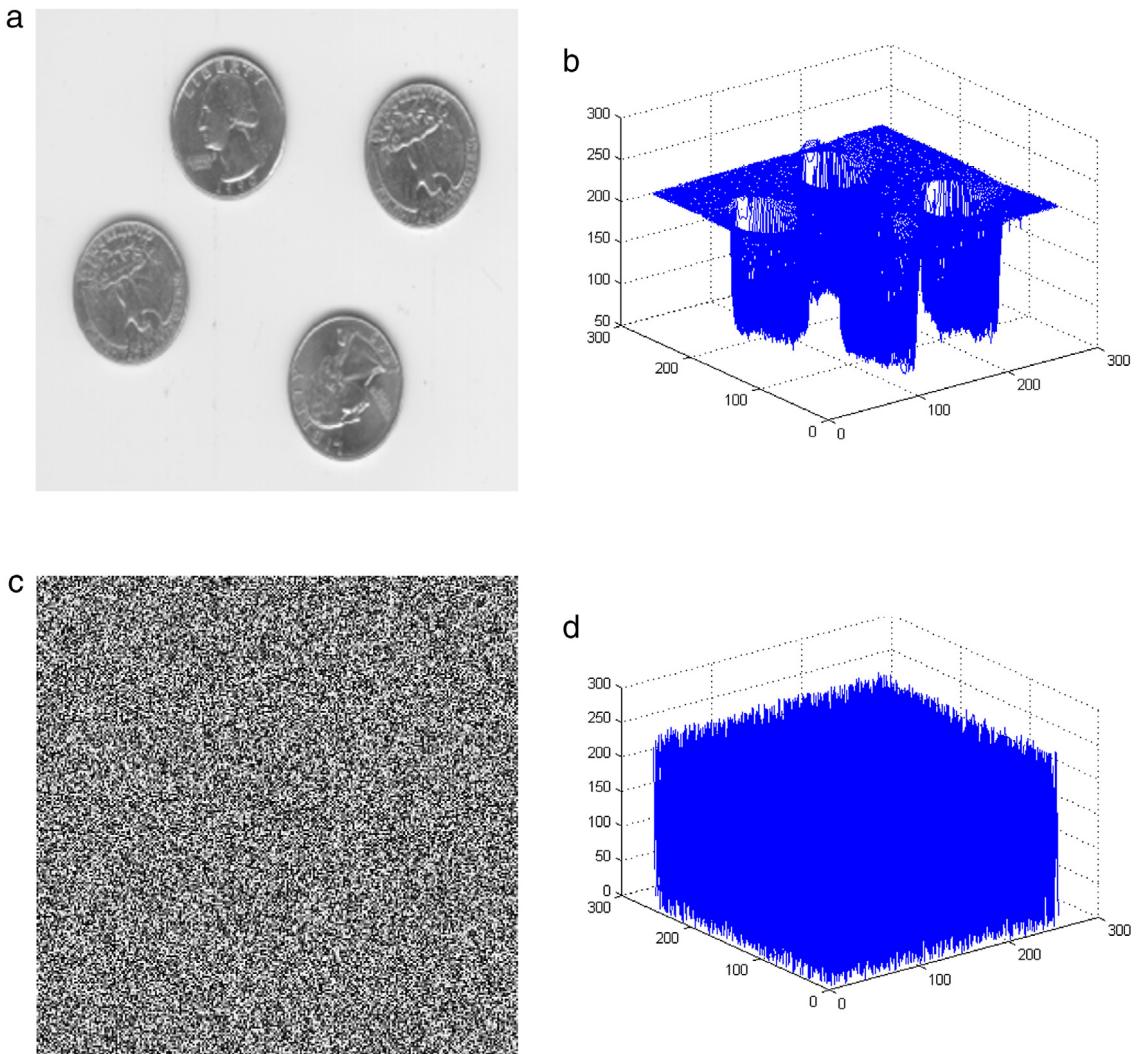


Fig. 9. Spatial characteristic analysis of eight image: (a) plain, (b) spatial, (c) ciphered, (d) spatial ciphered.

7. Conclusion

In this work, we have considered the Marotto's map represented in [25] in details in view of its dynamical analysis since it has not been investigated in any previous dynamical systems' work. Firstly, we have discussed the existence of fixed points and their local stability analysis. Secondly, a detailed co-dimension one bifurcation has been discussed using the center manifold theorem and bifurcation theory. The map has a variety of complex dynamics such as transcritical, flip and Neimark–Sacker bifurcations and we have reached explicit conditions for their occurrence. In addition, The map has been proven to be chaotic in the sense of Marotto. Numerical simulations agree with the theoretical analysis we obtained. Next, we have discussed the possibility of applying the map in image encryption since it has been investigated in many previous works that chaotic maps are well-fit and very promising for cryptography. The Marotto's map together with compound chaos and spatiotemporal chaos are combined as an encryption method. Finally, some test images are implemented to demonstrate the effectiveness of the proposed method.

Acknowledgments

The authors would like to thank the anonymous reviewers for providing some helpful comments which help to improve the original manuscript significantly. A special thanks to Prof. Dr. Yifeng Zheng for his help in the matlab code for encryption process.

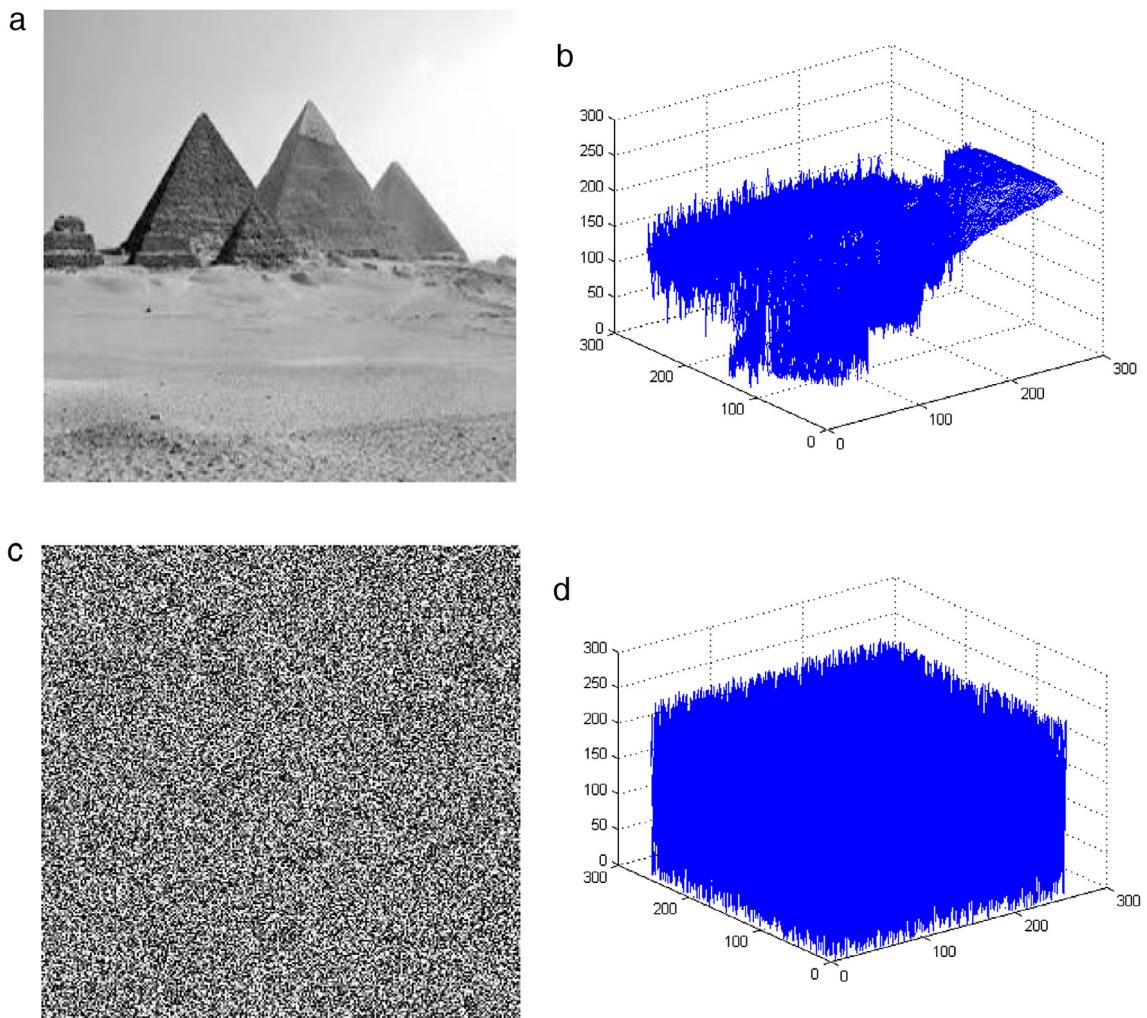


Fig. 10. Spatial characteristic analysis of pyramids image: (a) plain, (b) spatial, (c) ciphered, (d) spatial ciphered.

References

- [1] R.P. Agarwal, Difference Equations and Inequalities, second ed., in: Pure and Applied Mathematics, Chapman & Hall/CRC, New York, 2000.
- [2] D.G. Aronson, M.A. Chory, G.R. Hall, R.P. McGehee, A discrete dynamical system with subtly wild behavior, in: New Approaches To Nonlinear Problems in Dynamics (Proc. Conf. Pacific Grove, Calif. 1979), Vol. 359, SIAM, Philadelphia, PA, 1980, p. 339.
- [3] S. Elaydi, Is the world evolving discretely? *Adv. Appl. Math.* 31 (1) (2003) 1–9.
- [4] S. Elaydi, An Introduction to Difference Equations, third ed., Springer-Verlag, New York, 2005.
- [5] R. Holmgren, A First Course in Discrete Dynamical Systems, second ed., SpringerVerlag, New York, 1996.
- [6] W.G. Kelley, A.C. Peterson, Difference Equations, an Introduction with Applications, second ed., Academic Press, New York, 2000.
- [7] H. Sedaghat, Nonlinear difference equations, in: Theory with Applications to Social Science Models, Kluwer Academic, Dordrecht, 2003 Scientific, 1996.
- [8] G.I. Bischi, F. Tramontana, Three-dimensional discrete-time LotkaVolterra models with an application to industrial clusters, *Commun. Nonlinear Sci. Numer. Simul.* 15 (10) (2010) 3000–3014.
- [9] Z. Yicang, P. Fergola, Dynamics of a discrete age-structured SIS models, *Discrete Contin. Dyn. Syst. Ser. B* 4 (3) (2004) 843–852.
- [10] E. Ott, Chaos in Dynamical Systems, Cambridge University Press, Cambridge, 1993.
- [11] C. Mira, L. Gardini, A. Barugola, J.C. Cathala, Chaotic Dynamics in Two-Dimensional Noninvertible Maps, World scientific, Singapore, 1996.
- [12] G. Chen, S.T. Liu, On spatial periodic orbits and spatial chaos, *Internat. J. Bifur. Chaos Appl. Sci. Engrg.* 13 (3) (2003) 867–876.
- [13] G. Chen, S.T. Liu, On generalized synchronization of spatial chaos, *Chaos Solitons Fractals* 15 (2) (2003) 311–318.
- [14] S.T. Liu, G. Chen, On spatial lyapunov exponents and spatial chaos, *Internat. J. Bifur. Chaos Appl. Sci. Engrg.* 13 (5) (2003) 1163–1181.
- [15] S.T. Liu, G. Chen, Nonlinear feedback-controlled generalized synchronization of spatial chaos, *Chaos Solitons Fractals* 22 (4) (2004) 35–46.
- [16] S.T. Liu, G. Chen, Asymptotic behavior of delay 2-D discrete logistic systems, *IEEE Trans. Circuits Syst. I* 49 (11) (2002) 1677–1682.
- [17] G. Chen, C. Tian, Y. Shi, Stability and chaos in 2-D discrete systems, *Chaos Solitons Fractals* (25) (2005) 637–647.
- [18] C.P. Li, G. Chen, On the Marotto-Li-Chen theorem and its application to chaotification of multi-dimensional discrete dynamical systems, *Chaos Solitons Fractals* (18) (2003) 807–817.
- [19] F.Y. Sun, S.T. Liu, Spatial chaos-based image encrypti on design, *Sci. China Ser. G* 52 (2) (2009) 177–183.

- [20] F. Sun, S. Liu, Cryptographic pseudo-random sequence from the spatial chaotic map, *Chaos Solitons Fractals* 41 (5) (2009) 2216–2219.
- [21] E.M. Elabbasy, A.A. Elsadany, Y. Zhang, Bifurcation analysis and chaos in a discrete reduced Lorenz system, *Appl. Math. Comput.* 228 (2014) 184–194.
- [22] S.M. Salman, A.M. Yousef, A.A. Elsadany, Stability, bifurcation analysis and chaos control of a discrete predator-prey system with square root functional response, *Chaos Solitons Fractals* 93 (2016) 20–31.
- [23] C. Wang, X. Li, Further investigations into the stability and bifurcation of a discrete predator-prey model, *J. Math. Anal. Appl.* 422 (2) (2015) 920–939.
- [24] N. Romero, J. Silva, R. Vivas, On a coupled logistic map with large strength, *J. Math. Anal. Appl.* 415 (1) (2014) 346–357 Original Research Article.
- [25] F.R. Marotto, Snap-back repellers imply chaos in \mathbb{R}^n , *J. Math. Anal. Appl.* (63) (1978) 199–223.
- [26] T.Y. Li, J.A. Yorke, Period three implies chaos, *Amer. Math. Monthly* (82) (1975) 481–485.
- [27] C.S. Chen, T. Wang, Y.Z. Kou, X.C. Chen, X. Li, Improvement of trace-driven I-Cache timing attack on the RSA algorithm, *J. Syst. Softw.* (86) (2013) 100–107.
- [28] D. Coppersmith, The data encryption standard (DES) and its strength against attacks, *IBM J. Res. Dev.* (38) (1994) 243–250.
- [29] X.L. Huang, Image encryption algorithm using chaotic chebyshev generator, *Nonlinear Dynam.* (67) (2012) 2411–2417.
- [30] I. Hussain, T. Shah, Application of S-box and chaotic map for image encryption, *Math. Comput. Modelling* (57) (2013) 2576–2579.
- [31] A. Kanso, N. SmaouiX, Logistic chaotic maps for binary numbers generations, *Chaos Solitons Fractals* (40) (2013) 2557–2568.
- [32] H.J. Liu, X.Y. Wang, Color image encryption based on one-time keys and robust chaotic maps, *Comput. Math. Appl.* (59) (2010) 3320–3327.
- [33] M.A. Murillo-Escobar, C.C. Hernandez, F.A. Perz, R.M.L. Gutierrez, Acosta Del. Campo, OR a RGB image encryption algorithm based on total plain image characteristics and chaos, *Signal Process.* (109) (2015) 119–131.
- [34] N.K. Pareek, V. Patidar, K.K. Sud, Cryptography using multiple one-dimensional chaotic maps, *Commun. Nonlinear Sci. Numer. Simul.* (10) (2005) 715–723.
- [35] V. Patidar, N.K. Pareek, G. Purohit, K.K. Sud, Modified substitution-diffusion image cipher using chaotic standard and logistic maps, *Commun. Nonlinear Sci. Numer. Simul.* (15) (2010) 2755–2765.
- [36] F. Sun, Z. Lu, S. Liu, A new cryptosystem based on spatial chaotic system, *Opt. Commun.* (283) (2010) 2066–2073.
- [37] X.G. Tong, Z. Wang, M. Zhang, Y. Liu, H. Xu, J. Ma, An image encryption algorithm based on the perturbed high-dimensional chaotic map, *Nonlinear Dynam.* 80 (80) (2015) 1493–1508.
- [38] X.Y. Wang, K. Guo, A new image alternate encryption algorithm based on chaotic map, *Nonlinear Dynam.* 76 (2014) 1943–1950.
- [39] X.Y. Wang, D.P. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, *Commun. Nonlinear Sci. Numer. Simul.* 18 (2013) 3075–3085.
- [40] Y. Wang, K.K. Wong, X.F. Liao, T. Xiang, G.R. ChenX, A chaos-based image encryption algorithm with variable control parameters, *Chaos Solitons Fractals* (41) (2013) 1773–1783.
- [41] X. Wang, L. Teng, X. Qin, A novel color image encryption algorithm based on chaos, *Signal Process.* (93) (2012) 1101–1108.
- [42] X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, *Signal Process.* (92) (2012) 1101–1108.
- [43] K.W. Wong, S.W. Ho, C.K. Yung, A chaotic cryptography scheme for generating short ciphertext, *Phys. Lett. A* (310) (2003) 67–73.
- [44] G. Ye, K.W. Wong, An image encryption scheme based on time-delay and hyperchaotic system, *Nonlinear Dynam.* (71) (2013) 259–267.
- [45] S.S. Askar, A.A. Karawia, A. Alshamrani, Image encryption algorithm based on chaotic economic model, *Math. Probl. Eng.* (2015). <http://dx.doi.org/10.1155/2015/341729>.
- [46] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, *Chaos: Interdiscip. J. Nonlinear Sci.* 18 (2008). <http://dx.doi.org/10.1063/1.2959102>.
- [47] A. Skrobek, Cryptanalysis of chaotic stream cipher, *Phys. Lett. A* (363) (2007) 84–90.
- [48] D. Arroyo, J. Diaz, F.B. Rodriguez, Cryptanalysis of a one round chaos-based substitution permutation network, *Signal Process.* (93) (2013) 1358–1364.
- [49] C. Li, L. Zhang, R. Ou, K.W. Wong, S. Shu, Breaking a novel colour image encryption algorithm based on chaos, *Nonlinear Dynam.* (70) (2012) 2383–2388.
- [50] W. Yue, Y. Gelan, J. Huixia, Image encryption using the two-dimensional logistic chaotic map, *J. Electron. Imaging* 21 (1) (2012) 130–140.
- [51] S. Li, X. Mou, Y. Cai, On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision, *Comput. Phys. Comm.* 153 (1) (2003) 52–58.
- [52] C.X. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, *Opt. Commun.* 85 (1) (2012) 29–37.
- [53] T. Xiang, K.W. Wong, X.F. Liao, Selective image encryption using a spatiotemporal chaotic system, *Chaos* 17 (2) (2007). <http://dx.doi.org/10.1063/1.2728112>.
- [54] F.Y. Sun, S.T. Liu, Z.Q. Li, Z.W. Lu, A novel image encryption scheme based on spatial chaos map, *Chaos Solitons Fractals* 38 (3) (2008) 631–640.
- [55] F.Y. Sun, Z.W. Lu, S.T. Liu, A new cryptosystem based on spatial chaotic system, *Opt. Commun.* 283 (10) (2010) 2066–2073.
- [56] X. Tong, M. Cui, Image encryption with compound chaotic sequence cipher shifting dynamically, *Image Vis. Comput.* 26 (6) (2008) 843–850.
- [57] Z. Yifeng, J. Jianxiu, A novel image encryption scheme based on Hnon map and compound spatiotemporal chaos, *Multimedia Tools Appl.* (74) (2015) 7803–7820.
- [58] C.J.L. Albert, *Regularity and Complexity in Dynamical Systems*, Springer, New York, 2012.
- [59] Y. Kuznetsov, *Elements of Applied Bifurcation Theory*, third ed., Springer-Verlag, New York, 2004.
- [60] J. Guckenheimer, P. Holmes, *Nonlinear Oscillations, Dynamical System and Bifur- Cation of Vector Fields*, Springer-Verlag, New York, 1983.
- [61] F.R. Marotto, On redefining a snap-back repeller, *Chaos Solitons Fractals* (25) (2005) 25–28.