Dynamic Analysis and Cryptographic Application of a Sinusoidal-polynomial Composite Chaotic System

Hegui Zhu

Northeastern University College of Science

Jiangxia Ge

Northeastern University College of Science

Wentao Qi

Northeastern University College of Science

Xiangde Zhang

Northeastern University College of Science

Xiaoxiong Lu (✉ xiaoxionglu1@foxmail.com)

Xiangtan University <https://orcid.org/0000-0003-4493-7105>

Research Article

Keywords: 1D–sinusoidal polynomial composite chaotic system , Devaney chaos , image encryption , pixel segmentation , block chaotic matrix confusing

Posted Date: July 19th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-697808/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Dynamic Analysis and Cryptographic Application of a Sinusoidal-polynomial Composite Chaotic System

Hegui Zhu · Jiangxia Ge · Wentao Qi · Xiangde Zhang · Xiaoxiong Lu*

Received: 2021

Abstract Owing to complex properties of ergodicity, non-periodic ability and sensitivity to initial states, chaotic systems are widely used in cryptography. In this paper, we propose a sinusoidal-polynomial composite chaotic system (SPCCS), and prove that it satisfies Devaney's definition of chaos: the sensitivity to initial conditions, topological transitivity and density of periodic points. The experimental results show that the SPCCS has better unpredictability and more complex chaotic behavior than the classical chaotic maps. Furthermore, we provide a new image encryption algorithm combining pixel segmentation operation, block chaotic matrix confusing operation, and pixel diffusion operation with the SPCCS. Detailed simulation results verify effectiveness of the proposed image encryption algorithm.

Keywords 1D-sinusoidal polynomial composite chaotic system · Devaney chaos · image encryption · pixel segmentation · block chaotic matrix confusing

1 Introduction

Chaos is a sophisticated phenomena emerging in a deterministic system. In the past few decades, scientists found chaotic phenomena in many discipline, and chaotic systems have received universal attention [21, 23, 24,

32]. However, there hasn't been a strict and uniform mathematical definition of chaos yet. The most famous measure of chaos is Li-Yorke's chaos and Devaney's chaos, which are equivalent in some sense [5, 22]. With the development of chaos, people proposed many chaotic maps, such as Sine map, Chebyshev map, Logistic map and Tent map. Based on these classical chaotic maps, many kinds of variants were constructed [1, 2, 4, 6, 15, 17, 33]. Specifically, in [1], Ashish et al. provided rich dynamical chaotic behaviors by using a Mann iterative operation to Logistic map. In [13], Hua et al. generated 1D chaotic framework, which had better chaotic property than the used seed system. Furthermore, Hua et al. proposed the nonlinear chaotic structure containing six basic nonlinear operations with existing chaotic maps to generate a huge number of new chaotic maps in [14]. In these papers, the authors often tried to indicate the system's chaotic behavior by analyzing many mathematical experiments, however, the proof with computer simulation is not mathematically strict.

Moreover, using the definition of Li-Yorke's chaos or Devaney's chaos, many researchers have achieved significant results on dynamic analysis. For instance, Wu et al. proved that the lattice dynamical system was Li-Yorke chaotic for coupling constant $0 < \varepsilon < 1$ [34]. Luo et al. presented a homeomorphism and showed that an invertible mapping on a compact metric space was Li-Yorke chaotic [25]. Wang et al. provided two chaotic systems satisfying Devaney's definition of chaos in [29, 30]. In [38], Zheng et al. solved the chaotic dynamical degradation problem in real domain by providing an effective schemes with symbolic dynamics.

In fact, the improvement of chaos theory also has benefited image secure communication. The output of a chaotic system is sensitive to change of its parameter,

Hegui Zhu · Jiangxia Ge · Wentao Qi · Xiangde Zhang
College of Sciences, Northeastern University, Shenyang,
110819, China
Tel.: +86-24-83687680
E-mail: zhuhegui@mail.neu.edu.cn;

Xiaoxiong Lu(✉)
School of Computer Science, Xiangtan University, Xiangtan,
411105, China
E-mail: xiaoxiongglu1@foxmail.com;

non-periodic and unpredictable, which are consistent with the sensitivity requirement of a cryptographic system on secret key and the plaintext. Since Fridrich's chaotic encryption scheme analyzed in [36] was proposed in 1998, the corresponding research achievements have been growing rapidly [2, 8, 11, 12, 16, 19, 27, 31, 33, 37, 40, 41]. In [8], Guesmi et al. used DNA sequences and Lorenz chaotic system to enhance the information entropy of the proposed algorithm. Wang et al. proposed a high degree of security image communication scheme with Arnold coupled logistic map lattice model [31]. Due to the dynamics degradation of chaotic systems in finite-precision digital computer, the randomness of pseudo-random number sequence generated by iterating a chaotic system may be very low [18, 20, 28, 38]. In [9], Hu et al. proposed a new encryption scheme combining chaos with cycle operation for DNA sequences and obtained excellent diffusion properties. In [39], Zhou et al. proposed a novel 1D compound chaotic map with several simple chaotic maps. Ge et al. in [7] studied security of a feedback image encryption algorithm with rigorous mathematical proof. Besides, in [42], Zhu et al. also proposed an efficient image encryption algorithm with 2D hyper-chaotic system and local binary pattern, which had better security than ordinary chaotic-based encryption system.

In this paper, we propose a 1D sinusoidal polynomial composite chaotic system (SPCCS) combining Sine function with some special polynomial functions, and prove that the SPCCS satisfies Devaney's definition of chaos: the sensitivity to initial conditions, topological transitivity and periodic point density. To analyze the chaotic property of SPCCS, mathematical indexes such as bifurcation diagram, Lyapunov exponent and Correlation dimension are realized. The results show that SPCCS has excellent chaotic characteristics, and it is consistent with the theoretical analysis. The chaotic sequences generated by SPCCS are used for two rounds pixel segmentation operation, block chaotic matrix confusing operation, and pixel diffusion operation in the proposed image encryption algorithm. Experiments and simulation are provided to show the effectiveness of the theoretical analysis of the proposed algorithm.

The rest of the paper is organized as follows. A 1-D sinusoidal-polynomial composite chaotic system (SPCCS) is proposed in Sec. 2. Then, the proof of Devaney's definition of chaos of SPCCS is given in Sec. 3. Sec. 4 illustrates the chaotic performance of SPCCS with Chebyshev map and Sine map by some mathematical experiments. The proposed SPCCS-based image encryption algorithm is provided in Sec. 5. The encrypted performance and security analysis are presented in Sec. 6 and Sec. 7, respectively. Sec. 8 concludes the paper.

2 Sinusoidal-Polynomial Composite Chaotic System

As we know, Sine map can be denoted by

$$x_{n+1} = \mu \sin(\pi x_n).$$

If $\mu \in [0.87, 1]$, Sine map is chaotic. Especially, when $\mu = 1$, it is a self-map defined in $[0, 1]$. Similarly, Chebyshev map can be defined by

$$x_{n+1} = \cos(\lambda \arccos x_n).$$

If $\lambda > 1$, Chebyshev map has chaotic behaviors, and it is also a self-map defined in $[0, 1]$. Sine map and Chebyshev map are usually used as seed maps to apply various compound chaotic systems and chaotic encryption [39]. Then, we propose the sinusoidal-polynomial composite chaotic system (SPCCS)

$$f(x) = \sin(g(ax)), \quad (1)$$

where $a > 0$. Moreover, we assume that $g(x)$ satisfies the following assumptions:

- 1) $g(x)$ is a polynomial function with only odd terms and positive coefficients. Namely, $g(x) = \sum_{i=0}^n p_i x^i$, where $p_{2i} = 0$ and $p_{2i+1} \geq 0$.
- 2) a is a positive real number and satisfies $g(a) = k\pi$ ($k = 2, 3, \dots$) and

$$\frac{g'(a)}{g'(0)} \leq \frac{\pi}{2 \arcsin(\frac{1}{ag'(0)})} - 1. \quad (2)$$

Especially, for the inequality (2), we can flexibly adjust the value of p_1 to make the value of a wider.

Obviously, $f(x)$ is a self-map in $[0, 1]$. It should be noted that due to the mathematic complexity of the definition of Li-Yorkes chaos, Devaney's chaos is better than Li-Yorkes chaos in many special sense. In addition, we give the Theorem 1 and Theorem 2 to prove the Devaney's chaos of SPCCS $x_{n+1} = \sin(g(ax_n))$ in Sec. 3.

Theorem 1 If $[f^n(x)]' = 0$, then

$$f^n(x) = \begin{cases} \pm 1 & \text{if } n = 1; \\ 0, \text{ or } \pm 1 & \text{otherwise,} \end{cases}$$

where $f^n(x)$ denotes the n -th iteration of $f(x) = \sin(g(ax))$.

Proof : Since $f(x)$ is a continuous differentiable function, so $f^n(x)$ is differentiable. Let $f^0(x) = x$, then

$$[f^n(x)]' = \prod_{i=0}^{n-1} f'(f^i(x)),$$

So

$$\{x | [f^n(x)]' = 0\} = \bigcup_{i=0}^{n-1} \{x | f'(f^i(x)) = 0\}.$$

Referring to $f'(x) = a \cos(g(ax))g'(ax)$ and $|g'(ax)| \neq 0, a \neq 0$, that is

$$\bigcup_{i=0}^{n-1} \{x | [f^n(x)]' = 0\} = \bigcup_{i=0}^{n-1} \left\{x \mid g(af^i(x)) = \frac{\pi}{2} + l\pi\right\},$$

where $l \in \mathbb{N}$. Then, for $[f^n(x)]' = 0$, we consider the three situations:

- If $x \in \{x \mid g(af^{n-1}(x)) = \frac{\pi}{2} + l\pi\}$, then

$$f^n(x) = f(f^{n-1}(x)) = \sin\left(\frac{\pi}{2} + l\pi\right) = \pm 1.$$

- If $x \in \{x \mid g(af^{n-2}(x)) = \frac{\pi}{2} + l\pi\}$, then

$$f^n(x) = f(\sin(g(af^{n-2}(x)))) = \sin(g(\pm a)) = 0.$$

- If $x \in \bigcup_{i=0}^{n-3} \{x \mid g(af^i(x)) = \frac{\pi}{2} + l\pi\}$, then

$$f^{i+2}(x) = f(\sin(g(af^i(x)))) = \sin(g(\pm a)) = 0,$$

where $0 \leq i \leq n-3$. So

$$f^n(x) = f^{n-i-2}(f^{i+2}(x)) = f^{n-i-2}(0) = 0.$$

Thus, with the above discussion, this concludes the proof.

Theorem 2 For any $x \in [-1, 1]$, If $|f'(x)| \leq 1$, then

$$|f'(f(x))| > 1.$$

Proof : Firstly, we divide interval $[-1, 1]$ into two disjoint sets:

$$X_1 = \{x \mid |f'(x)| > 1\},$$

$$X_2 = \{x \mid |f'(x)| \leq 1\}.$$

Because $f(x) = \sin(g(ax))$ is an origin-symmetric odd polynomial function, we only need to prove Theorem 2 in $[0, 1]$. Suppose $x_1, x_2, \dots, x_n$ are the extreme point of $f(x)$ in $[0, 1]$ and $x_1 < x_2, \dots, < x_n$, then $f'(x_i) = 0$, where $i = 1, 2, \dots, n$. Due to $f = \sin(g(ax))$, in the neighborhood of each extreme point x_i , there are x_i^- and x_i^+ ($x_i^- < x_i < x_i^+$) such that $|f'(x_i^+)| = 1$ and $|f'(x_i^-)| = 1$ and $[x_i^-, x_i^+] \subset X_2$. Thus, one has

$$\begin{cases} |f'(x_i^-)| = |a \cdot \cos(g(ax_i^-)) \cdot g'(ax_i^-)| = 1; \\ |f'(x_i^+)| = |a \cdot \cos(g(ax_i^+)) \cdot g'(ax_i^+)| = 1. \end{cases} \quad (3)$$

Based on the Eq. (3) and $g''(x) \geq 0$, one can get

$$|\cos(g(ax_i^+))| < |\cos(g(ax_i^-))|.$$

So $g(ax_i^+) - g(ax_i) < g(ax_i) - g(ax_i^-)$, then due to $a > 0$, one has

$$x_i^+ - x_i < x_i - x_i^-. \quad (4)$$

Similarly, for the different extreme points x_i and x_{i+1} , one can obtain

$$x_{i+1} - x_{i+1}^- < x_i^+ - x_i, \quad (5)$$

from $|f'(x_i^+)| = 1$ and $|f'(x_{i+1}^-)| = 1$. Especially, x_1 and x_n are respectively the first and last extreme points of $f(x)$ in $[0, 1]$, so $g(ax_1) = \frac{\pi}{2}$ and $g(ax_n) = k\pi - \frac{\pi}{2}$. To facilitate the above the discussion, draw the situation in the neighborhood of the first two extreme points and the last extreme point $f(x)$ shown in Fig. 1. According

Fig. 1 The curve of $f(x)$

to Eqs. (4) and (5), one has

$$x_1 - x_1^- > x_1^+ - x_1 > x_i - x_i^- > x_i^+ - x_i,$$

where $i = 2, 3, \dots, n$. For any x_i , according to Lagrange's median value theorem and $[x_i^-, x_i^+] \subset X_2$, one has

$$\begin{cases} 1 - f(x_i^-) < x_i - x_i^- < x_1 - x_1^-; \\ 1 - f(x_i^+) < x_i^+ - x_i < x_1 - x_1^+. \end{cases}$$

If we can proof $x_1 - x_1^- < 1 - x_n^+$, then the above equation becomes

$$\begin{cases} 1 - f(x_i^-) < 1 - x_n^+; \\ 1 - f(x_i^+) < 1 - x_n^+. \end{cases}$$

Meanwhile, one can obtain $(f(x_i^-), 1) \subset (x_n^+, 1)$ and $(f(x_i^+), 1) \subset (x_n^+, 1) \subset X_1$, so the theorem is proved.

Now, we turn to proof $x_1 - x_1^- < 1 - x_n^+$. Setting $i = x_1$ and $i = x_n$ in Eq. (3), one can get $|\cos(g(ax_1^-))| > |\cos(g(ax_n^+))|$, and

$$\frac{\pi}{2} - g(ax_1^-) > g(ax_n^+) - (k\pi - \frac{\pi}{2}) \quad (6)$$

From $g''(x) > 0$, one can obtain $x_1 - x_1^- < \frac{\frac{\pi}{2} - g(ax_1^-)}{ag'(0)}$ and $\frac{k\pi - g(ax_n^+)}{ag'(a)} < 1 - x_n^+$. If

$$\frac{g'(a)}{g'(0)} < \frac{k\pi - g(ax_n^+)}{\frac{\pi}{2} - g(ax_1^-)}. \quad (7)$$

holds, one has $x_1 - x_1^- < 1 - x_n^+$ and

$$\frac{\frac{\pi}{2} - g(ax_1^-)}{ag'(0)} < \frac{k\pi - g(ax_n^+)}{ag'(a)}. \quad (8)$$

It can be seen that the Eq. (8) is equivalent to Referring to Eq. (6) and Eq. (7), one has

$$\frac{k\pi - g(ax_n^+)}{\frac{\pi}{2} - g(ax_1^-)} = \frac{\frac{\pi}{2} - (g(ax_n^+) - (k\pi - \frac{\pi}{2}))}{\frac{\pi}{2} - g(ax_1^-)} > \frac{\frac{\pi}{2} - \alpha}{\alpha},$$

where $\alpha = \pi/2 - g(ax_1^-)$ and $\alpha \in (0, \pi/2)$. Substituting $i = 1$ in the Eq. (3), one can get $\alpha < \arcsin(\frac{1}{ag'(0)})$, thus

$$\frac{\frac{\pi}{2} - \alpha}{\alpha} > \frac{\pi}{2 \arcsin(\frac{1}{ag'(0)})} - 1.$$

According to the inequality (2), one can know that Eq. (7) holds, thus $x_1 - x_1^- < 1 - x_n^+$.

3 The Proof of SPCCS by Devaney's Definition of Chaos

In this Section, we will prove SPCCS satisfies Devaney's definition of chaos.

3.1 Sensitivity dependence on initial conditions

Firstly, we divide the interval $[-1, 1]$ into two disjoint sets X_1 and X_2 :

$$X_1 = \{x \mid |f'(x)| > 1\},$$

$$X_2 = \{x \mid |f'(x)| \leq 1\}.$$

Then, we discuss the sensitivity dependence on the interval X_1 and X_2 , respectively.

(1) For every $x_0 \in X_1$, $\varepsilon > 0$, there exists an integer $k_1 > [\frac{1}{\varepsilon}] + 1$ satisfying $x_1 = x_0 + \frac{1}{k_1} \in U(x_0, \varepsilon)$ and $(x_0, x_1) \subset U(x_0, \varepsilon)$, where $[\cdot]$ is an integer quantization function. Since $f'(x)$ is continuous, there exists $k_2 > 0$ such that $x_2 = x_0 + \frac{1}{k_2} \in X_1$ and $(x_0, x_2) \subset X_1$. Setting $k_* = \max(k_1, k_2)$, then there is

$$x_3 = x_0 + \frac{1}{k_*}$$

satisfies $(x_0, x_3) \subset X_1$ and $(x_0, x_3) \subset U(x_0, \varepsilon)$. Thus, for any given $\varepsilon > 0$, when $k > k_*$, one can get

$$|f(x_3) - f(x_0)| = |f'(\xi)| |x_3 - x_0| = |f'(\xi)| \frac{1}{k_*} > \frac{1}{k},$$

where $\xi \in (x_0, x_3)$. That is $|f^n(x_3) - f^n(x_0)| > \delta$ with $\delta = \frac{1}{k}$ and $n = 1$.

(2) Now we turn to X_2 , for every $x'_0 \in X_2$ and $\varepsilon > 0$, set $k'_1 > [\frac{1}{\varepsilon}] + 1$ and then $x'_1 = x'_0 + \frac{1}{k'_1} \in U(x'_0, \varepsilon)$. Because $f'(x)$ is continuous, there exists $k'_2 > 0$ such that $x'_2 = x'_0 + \frac{1}{k'_2} \in X_2$ and $(x'_0, x'_2) \subset X_2$. Let $k'_* = \max(k'_1, k'_2)$, then there must be

$$x'_3 = x'_0 + \frac{1}{k'_*}$$

satisfies $(x'_0, x'_3) \subset X_2$ and $(x'_0, x'_3) \subset U(x'_0, \varepsilon)$. Referring to Theorem 2, one can get $f(x'_0), f(x'_3) \in X_1$. Without loss of generality, assuming that $f(x'_0) < f(x'_3)$, then for any $\eta \in (f(x'_0), f(x'_3))$, one can know there is a $\theta \in (x'_0, x'_3)$ such that $f(\theta) = \eta$ from the intermediate value theorem of continuous function. So, $\eta \in X_1$ and $(f(x'_0), f(x'_3)) \subset X_1$. Thus, for any given $\varepsilon > 0$, when $k > k'_*$, one has

$$\begin{aligned} |f^2(x'_3) - f^2(x'_0)| &= |f(f(x'_3)) - f(f(x'_0))| \\ &= |f'(f(z))| \cdot |f(x'_3) - f(x'_0)| \\ &> |f(x'_3) - f(x'_0)| \end{aligned}$$

where $f(z) \in (f(x'_0), f(x'_3))$. That is $|f^n(x_3) - f^n(x_0)| > \delta$ with $\delta = |f(x'_3) - f(x'_0)|$ and $n = 2$.

In conclusion, for any $x \in [-1, 1]$, the function $f(x)$ satisfies the sensitivity dependence on initial conditions.

3.2 Topological transitivity

Let X_k^1 and X_k^2 be the maximum and minimum points set of k -th ($k = 1, 2, \dots$) iteration of $f(x)$, respectively. Then $X_1^k = \{x \mid f^k(x) = 1\}$ and $X_2^k = \{x \mid f^k(x) = -1\}$. The elements of X_1^k and X_2^k are arranged in ascending order, we have $X_1^k = \{x_{11}^k, x_{12}^k, \dots, x_{1p_k}^k\}$ and $X_2^k = \{x_{21}^k, x_{22}^k, \dots, x_{2p_k}^k\}$, where p_k is a positive integer. Setting that $d_1^k = \max_{1 \leq j \leq p_k-1} \{x_{1,j+1}^k - x_{1j}^k\}$, $d_2^k = \max_{1 \leq i \leq p_k-1} \{x_{2,i+1}^k - x_{2i}^k\}$ and $d^k = \max_{1 \leq i \leq p_k-1} \{d_1^k, d_2^k\}$. Then $d^k = d_1^k = d_2^k$ because the elements in X_1^k and X_2^k are origin-symmetric. Without loss of generality, we only consider d_2^k corresponding to X_2^k in the following.

Take two adjacent $x_{2i_0}^k, x_{2,i_0+1}^k \in X_2^k$ and satisfy $d_2^k = x_{2,i_0+1}^k - x_{2i_0}^k$, then $f'(x_{2i_0}^k) = f'(x_{2,i_0+1}^k) = 0$, where $k = 2, 3, \dots$. According to Theorem 1 and $f(\pm 1) = \sin(g(\pm a)) = 0$, there are only two types curves of $f^k(x)$ between $x_{2i_0}^k$ and x_{2,i_0+1}^k which are shown in Fig. 2. Due to $X_2^{k+1} = \{x \mid f^{k+1}(x) = -1\}$, we can know $X_2^{k+1} = \{x \mid f^k(x) \in X_2^1\}$. Only extract one point $x_{2r_0}^1 \in X_2^1$, then there are $x_{2j}^{k+1}, x_{2,j+s_0}^{k+1} \in X_2^{k+1}$ satisfying $f^k(x_{2j}^{k+1}) = f^k(x_{2,j+s_0}^{k+1}) = x_{2r_0}^1$, where $s_0 \geq 1$. With the increasing of iterations times k , the

Fig. 2 Two types of $f^k(x)$ between $x_{2i_0}^k$ and $x_{2i_0+1}^k$. (a) 0 is not extreme value; (b) 0 is the extremum value.

curves of $f^k(x)$ are approximated as broken lines that shown in Fig. 3. Observing Fig. 3a, one can get

$$\frac{1 - x_{2r_0}^1}{2} d_2^k = |x_{2j}^{k+1} - x_{2j+s_0}^{k+1}| \leq s_0 \cdot d_2^{k+1}.$$

So, it implies that $\lim_{k \rightarrow +\infty} d_2^k = \lim_{k \rightarrow +\infty} \left(\frac{1-x_{2r_0}^1}{2 \cdot s_0}\right)^{k-1} \cdot d_2^1 = 0$. Similarly, we can know $\lim_{k \rightarrow +\infty} d_2^k = 0$ from Fig. 3b.

So $\lim_{k \rightarrow +\infty} d^k = 0$

Fig. 3 Approximate broken line treatment of Fig. 2. (a) 0 is not extreme value; (b) 0 is extreme value.

In conclusion, with the increasing of iterations times k , the number of extreme points increases gradually. Then for any open interval $U \subset [-1, 1]$, there exists a positive integer k such that $d(U) > d_k$ and $f^k(U) = [-1, 1]$. Therefore, $f^k(U) \cap V \neq \emptyset$ for any open interval $V \subset [-1, 1]$, this completes the proof.

3.3 Density of the periodic points

Observing the proof of topological transitivity, for any open interval $U \subset [-1, 1]$, there exists $k > 0$ satisfying $d(U) > d^k$. It means that there are at least two adjacent maximum or minimum points in U . Thus, there are at least two points in the interval U satisfying $x = f^k(x)$. Due to the arbitrariness of interval U , the

periodic points are dense in the whole interval $[-1, 1]$, and this completes the proof.

4 Numerical simulations

In this section, we propose two specific examples of SPCCS called S-P1 map and S-P2 map with $a \in [0, 3]$ in Table 1. The chaotic behaviors are compared with Chebyshev chaotic map and Sine chaotic map in Subsection 4.1, Subsection 4.2 and Subsection 4.3, respectively.

Table 1 Four chaotic maps.

Chaotic map	Mathematical expression
Sine map	$x_{n+1} = a \sin(\pi x_n)$
Chebyshev map	$x_{n+1} = \cos(a \cdot \arccos x_n)$
S-P1 map	$x_{n+1} = \sin(\pi a^3 x_n^3 + 10\pi a x_n)$
S-P2 map	$x_{n+1} = \sin(\pi a^5 x_n^5 + \pi a^3 x_n^3 + 10\pi a x_n)$

4.1 Bifurcation diagram

According to the dynamical system theory, the bifurcation phenomenon is a symbol of chaos. In this subsection, the bifurcation diagrams of Sine map, Chebyshev map, S-P1 map and S-P2 map are illustrated in Fig. 4. As can be seen from Fig. 4, the output of S-P1 map and S-P2 map have larger chaotic area than Sine map and Chebyshev map.

Fig. 4 Bifurcation diagram. (a) Sine map; (b) Chebyshev map; (c) S-P1 map; (d) S-P2 map.

4.2 Lyapunov exponent

The Lyapunov exponent describes the orbit produced by two very similar initial values in the phase space [19, 34]. The average rate of dispersion or convergence of Lyapunov exponent (LE) is an important index to judge chaos. Here, we depict the Lyapunov exponent spectrum of the Sine map, Chebyshev map, S-P1 map and S-P2 map in Fig. 5 with $a \in [0, 3]$. Moreover, the corresponding maximum Lyapunov exponent and average Lyapunov calculation results are also listed in Table 2. All these results demonstrate that the S-P1 map and S-P2 map have larger Lyapunov exponent and average Lyapunov exponent, and have better chaotic and random performance.

Fig. 5 Lyapunov exponents for different maps.

Table 2 Lyapunov exponent results

Chaotic map	Maximum LE	Average LE
Sine map	1.7570	0.0742
Chebyshev map	1.1627	0.4451
S-P1 map	4.6106	3.1969
S-P2 map	5.9486	3.8667

4.3 Correlation dimension

Correlation dimension (CD) is applied to illustrate the singularity of attractors in dynamical system [25]. Let $S = \{s_1, s_2, \dots\}$ be a time series and e be embedded dimension, then CD of the S is computed by

$$d = \lim_{r \rightarrow 0} \lim_{N \rightarrow \infty} \frac{\log C_e(r)}{\log r},$$

Fig. 6 The values of Correlation dimension for different maps.

$$C_e(r) = \lim_{N \rightarrow \infty} \frac{\sum_{i=1}^{N-(e-1)\zeta} \sum_{j=i+1}^{N-(e-1)\zeta} \theta(r - |\bar{s}_i - \bar{s}_j|)}{[N - (e-1)\zeta][N - (e-1)\zeta - 1]},$$

where $\theta(\cdot)$ is the Heaviside step function and ζ is time delay. And $\bar{s}_t = (s_t, s_{t+\zeta}, s_{t+2\zeta}, \dots, s_{t+(e-1)\zeta})$, $t = 1, 2, \dots, N - (e-1)\zeta$. Generally, the embedding dimension $e = 2$ and time delay $\zeta = 1$ for a 1-D system [26]. Then the CD values of different systems are drawn in Fig. 6. From Fig. 6, it can be seen that the S-P1 map and S-P2 map have more stable correlation dimension values and larger parameter change fields. Meanwhile, the S-P1 map and S-P2 map have higher maximum and average correlation dimension values with $a \in [0, 3]$. Therefore, the phase space of the S-P1 map and S-P2 map have excellent chaotic performance.

5 The encryption algorithm

In this section, we propose a SPCCS-based image encryption algorithm, which includes pixel segmentation operation, and two rounds of block chaotic matrix confusing operation and Pixel diffusion operation. Its detailed contents are described as follows:

For an image P with size of $M \times N$, firstly, we divide it into an image H with size of $2^k \times 2^l$ ($k \leq l$) by the pixel segmentation operation. Then, the image H is divided into blocks of size $2^{k-1} \times 2^{l-1}$. And the confused image U is obtained by block chaotic matrix generated with SPCCS for each block of image H . Finally, the cipher image W generated by the first round of the pixel diffusion operation is used as the H of the second round of the block chaotic matrix confusing operation, and the final W is obtained after the second round of pixel diffusion operation. The encryption algorithm flow chart is shown in Fig. 7.

Fig. 7 The image encryption algorithm.

5.1 Pixel segmentation

The detailed steps of the pixel segmentation operation are shown as follows.

Step 1: For a plain image P with size of $M \times N$, choose the integers $k, l, (k \leq l)$ that $2^{k-1} < M \leq 2^k$, $2^{l-1} < N \leq 2^l$.

Step 2: Randomly select the initial values x_1, x_2 and the control parameters a_1, a_2 of SPCCS that satisfy condition 2), and iterate $2^k \times 2^l + 2000$ times to obtain two chaotic sequences s_1, s_2 , where the first 2000 outputs are discard to avoid the harmful effect of SPCCS, then obtain two integer sequences S_1, S_2 by

$$\begin{cases} S_1 = \text{floor}(s_1 \times 2^{16}) \bmod 8, \\ S_2 = \text{floor}(s_2 \times 2^{16}) \bmod 8. \end{cases} \quad (9)$$

Step 3: Suppose $m = 2^k - M$, so $m < M$. Firstly, for each pixel value x from $M - m + 1$ to M row of plain image P , we turn it into a 8 bits binary sequence and divide it into two pixel values by

$$\begin{cases} t_1 = CL(x, S_1(i)), \\ t_2 = CR(x, S_1(i)). \end{cases} \quad (10)$$

Then we concatenate t_1, t_2 vertically, and get an intermediate image T with size of $2^k \times N$, where $CL(x, S_1(i))$ represents to circleleft shift x with chaotic number $S_1(i)$, $CR(x, S_1(i))$ represents to circle right shift x with chaotic number $S_1(i)$.

Step 4: Suppose $n = 2^l - N$, so, $n < N$. For each pixel value y from column $N - n + 1$ to N of image T , we divide it into two pixel values by

$$\begin{cases} y_1 = CL(y, S_2(i)), \\ y_2 = CR(y, S_2(i)). \end{cases} \quad (11)$$

Then we concatenate y_1, y_2 horizontal and obtain the permuted image H of size $2^k \times 2^l$.

For an image P of size 3×4 . Considering $2 < 3 < 2^2$ and $4 = 2^2$, we divide the 3rd row of image P to get an image with size of 4×4 . Suppose the chaotic sequence $S_1 = \{4, 6, 7, 2\}$. Fig. 8 illustrates a numeral example

of the Pixel segmentation operation by Step 3. From Fig. 8, it can be conclude that the size and pixel values of plain image have been changed.

Fig. 8 An example of Pixel segmentation operation.

5.2 Block chaotic matrix confusing operation

After the pixel segmentation operation, we do block chaotic matrix confusing operation in this subsection, the detailed steps are illustrated as follows.

Step 1: For image H obtained in Subsection 5.1, we truncate it into $q = 2^{l-k+2}$ image blocks $[K_t]_{t=1}^q$ with size of $2^{k-1} \times 2^{k-1}$ from left to right and top to bottom.

Step 2: Randomly select the initial value x_3 and the control parameter a_3 of SPCCS that satisfy condition 2). Then we iterate $2^k \times 2^l + 2000$ times to obtain a chaotic sequence s_3 , and obtain an integer sequence S_3 by

$$S_3 = \text{floor}(s_3 \times 2^{16}) \bmod 256.$$

Step 3: Use the sequence S_3 to get the initialized image matrix $[V_t]_{t=1}^q$ from left to right and top to bottom. Then, we sort each row of V_t and obtain corresponding index matrices $[D_t]_{t=1}^q$.

Step 4: Construct a new index matrix Q_t with the index matrix D_t by

$$Q_t = \begin{bmatrix} (D_t(1,1),1) & \cdots & (D_t(1,2^{k-1}),1) \\ (D_t(2,1),2) & \cdots & (D_t(2,2^{k-1}),2) \\ \vdots & & \vdots \\ (D_t(2^{k-1},1),2^{k-1}) & \cdots & (D_t(2^{k-1},2^{k-1}),2^{k-1}) \end{bmatrix}.$$

Then, we can obtain the blocked confused image $[G_t]_{t=1}^q$ with size of $2^{k-1} \times 2^{k-1}$ by

$$G_t(D_t(i,j),i) = K_t(D_t(i+1,j),i+1)$$

and

$$G_t(D_t(2^{k-1}, j), 2^{k-1}) = K_t(D_t(1, j), 1),$$

where $1 \leq i \leq 2^{k-1} - 1$, $1 \leq j \leq 2^{k-1}$.

Step 5: For $i = 1$ to q , repeat Step 4, and generate the confused image matrix U with size of $2^k \times 2^l$.

To facilitate the understanding of steps 3 and 4, a simple numerical example is described through Fig. 9 and 10. Fig. 9 shows a numeral example of how to generate the new index matrix Q_t with size of 4×4 in Step 4. It can be observed that the first row of D_t is $(2, 4, 3, 1)$, so the first row of new index matrix Q_t is $((2, 1), (4, 1), (3, 1), (1, 1))$. The second row of D_t is $(3, 2, 4, 1)$, so the second row of new index matrix Q_t is $((3, 2), (2, 2), (4, 2), (1, 2))$, and so on. Fig. 10 shows

Fig. 9 An example of how to generate the new index matrix Q_t .

a numeral example of how to obtain the blocked confused image G_t from Q_t in Fig. 9. In index matrix Q_t , $(1, 1)$, $(1, 2)$, $(1, 3)$ and $(1, 4)$ corresponds to $(1, 2)$, $(2, 3)$, $(2, 4)$ and $(1, 1)$, respectively. So, $G_t(1, 1) = K_t(1, 2)$, $G_t(1, 2) = K_t(2, 3)$, $G_t(1, 3) = K_t(2, 4)$, $G_t(1, 4) = K_t(1, 1)$, and so on. Thus, image G_t can be indicated in Fig. 10.

Fig. 10 An example of how to obtain the blocked confused image G_t from Q_t in Fig. 9.

5.3 Pixel diffusion

After the block chaotic matrix confusing operation, in this subsection, we will show the detailed pixel diffusion procedure.

Step 1: Randomly select the initial values x_4, x_5 and control parameters a_4, a_5 of SPCCS that satisfy condition 2), and iterate $2^k \times 2^l + 2000$ times to obtain chaotic sequences s_4, s_5 , then get two integer sequences S_4, S_5 by

$$\begin{cases} S_4 = \text{floor}(s_4 \times 2^{16}) \bmod 256, \\ S_5 = \text{floor}(s_5 \times 2^{16}) \bmod 256. \end{cases}$$

Step 2: Rearrange S_4, S_5 to two matrices J_1, J_2 with size of $2^k \times 2^l$, respectively.

Step 3: Randomly select integer $r_1 \in [0, 255]$, and do Step3 and Step 4, then

$$W(1, 1) = (U(1, 1) + J_1(1, 1) + r_1) \bmod 256, \quad (12)$$

where U is the confused image matrix with size of $2^k \times 2^l$.

Step 4: For $j=2$ to $2^l - 1$, we calculate

$$W(1, j) = (U(i, j) + W(1, j-1) + J_1(1, j)) \bmod 256. \quad (13)$$

Step 5: For $i = 2$ to 2^k , $j = 1$ to 2^l , we diffuse the next $2^k - 1$ rows of image U by

$$\begin{cases} U' = \sum_{s=1}^{2^l} W(i-1, s), \\ W(i, j) = (U(i, j) + U' + J_1(i, j)) \bmod 256. \end{cases} \quad (14)$$

Step 6: Compute $W = W \oplus J_2$ and obtain W .

6 Simulation results

In this section, to illustrate the encryption performance of the proposed SPCCS-based encryption algorithm. Many different kinds of images such as gray value images, color images and binary images are chosen from USB-SIPS image database and Brown Univ Large Binary image database to do the encryption quality and encryption time analysis.

6.1 Encryption quality

Obviously, the proposed image algorithm should have outstanding encryption performances in different kinds of images. Fig. 11 shows the encryption effect of binary image, gray image, monochrome image and color images, respectively. Fig. 11c shows that all the plain images are encrypted to a random-like image. Moreover, as show in Fig. 11d, the histogram of cipher images are uniformly distributed that verify the encrypted effect, and the attackers can't obtain meaningful information about the plain images.

Fig. 11 Simulation results. (a) the binary, gray, monochrome and color images; (b) histograms of (a); (c) encrypted results of (a); (d) histograms of (c); (e) decrypted results of (c).

6.2 Encryption time performance

The running time of a good image encryption algorithm must be acceptable for different scenario [21]. From Table 3, the encryption time of the proposed algorithm is much lower than that of the three comparable algorithms for different scenario, it shows the proposed encryption algorithm can be a good choice for practical application.

Table 3 Encryption time performance(s)

Image size	Ours	[42]	[39]	[2]
256 × 256	0.310971	0.702159	1.559948	14.599061
512 × 512	1.224121	2.694952	6.128348	58.902637

7 Security analysis

An ideal image encryption algorithm must can pass several security analysis, and if SPCCS-based image encryption algorithm fails one of the security index, it means the SPCCS-based algorithm cannot be used for real application. Here, different kinds of security analysis for the SPCCS-based algorithm are depicted.

7.1 Histogram analysis

From the perspective of statistics, the histogram of cipher image must be flat. Fig. 11 shows the histograms of

the white-black image, gray image, monochrome image and color image, respectively. As shown in Fig. 11, the histograms of their encrypted images are all uniform distributions, so, it is enough to resist statistic attacks for universal image.

7.2 Correlation analysis

Generally, image data has high redundancy of data and strong correlation among neighboring pixels, which is meaningful for attackers. Then, we choose 1000 pairs of adjacent pixels from plain and encrypted images, and analyze the correlations at horizontal, vertical and diagonal directions, respectively. The correlation coefficient is calculated by

$$r = \frac{|E((x_1 - E(x_1))(x_2 - E(x_2)))|}{\sqrt{D(x_1)D(x_2)}}, \quad (15)$$

where $E(\bullet)$ and $D(\bullet)$ are the expectation and variance operation of a random variable.

The correlation diagram and correlation coefficients are shown in Fig. 12 and Table 4, respectively. In Fig. 12 and Table 4, the correlation coefficient of cipher image is very close to 0. It implies that the correlation of the plain image is eliminated in encrypted image.

Fig. 12 Correlation analysis of image Lena. (a) Horizontal, vertical, and diagonal direction of original images; (b) Horizontal, vertical, and diagonal direction of encrypted images.

7.3 Local Shanny entropy

Except for information entropy, Local Shanny entropy (LSE) is another norm for measuring randomness [35]. It is computed by

$$H_s(P) = - \sum_{i=1}^t \frac{H(P_i)}{s},$$

Table 4 Pixel correlations of the original image and its encrypted image

Image	Plaintext			Ciphertext		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
6.1.01	0.9910	0.9860	0.9712	0.0118	0.0177	0.0088
7.1.08	0.9180	0.9601	0.9188	0.0183	-0.0048	0.0183
Boat.512	0.9720	0.9340	0.9183	0.0036	0.0085	-0.0127
4.2.03(r)	0.8597	0.9243	0.8435	0.0020	0.0319	0.0105
4.2.03(g)	0.7699	0.8620	0.7462	0.0109	-0.0410	-0.0257
4.2.03(b)	0.8900	0.9069	0.8374	0.0252	0.0513	0.0247

where P_i is a randomly non-overlapping block of cipher image, $H(P_i)$ is the information entropy of block P_i . For an ideal image encryption, $H_s(P)$ should fall into (7.901515698, 7.903422936) with significance $\alpha=0.001$, $s = 30$ and $t = 1936$. Table 5 shows the LSE results of SPCCS-based algorithm and three comparable algorithms. The SPCCS-based algorithm has 19 test images pass LSE test, which means the SPCCS-based algorithm has a good performance in randomness.

Table 5 LSE analysis

Image	Ours	[42]	[39]	[2]
5.1.09	7.901662	7.904797	7.897780	7.901975
5.1.10	7.904019	7.899908	7.902330	7.903907
5.1.11	7.902317	7.904016	7.902062	7.904037
5.1.12	7.903962	7.902356	7.900694	7.904959
5.1.13	7.902219	7.900514	7.899931	7.900331
5.1.14	7.906935	7.901753	7.899931	7.903424
5.2.08	7.902375	7.902602	7.902969	7.903776
5.2.09	7.902650	7.902807	7.901872	7.901885
5.2.10	7.903289	7.904108	7.903584	7.903903
7.1.01	7.902923	7.902189	7.901535	7.904415
7.1.02	7.903197	7.903810	7.904993	7.901124
7.1.03	7.902679	7.902906	7.901278	7.903624
7.1.04	7.903298	7.905187	7.901918	7.902831
7.1.05	7.902369	7.901569	7.902774	7.902889
7.1.06	7.902896	7.903455	7.905048	7.902413
7.1.07	7.902586	7.901996	7.902274	7.904307
7.1.08	7.903234	7.903497	7.902100	7.903705
7.1.09	7.902105	7.901653	7.903076	7.903354
boat.512	7.902309	7.903291	7.901361	7.900266
house(r)	7.903181	7.901158	7.902090	7.902349
house(g)	7.902681	7.901530	7.899425	7.902349
house(b)	7.903168	7.902178	7.904330	7.903480
Pass rate	19/22	12/22	11/22	7/22

slightly change of key. From Fig. 13 and Fig. 14, it can be known that the proposed SPCCS-based algorithm is very sensitive to tiny change of key, which is most important for image communication. Furthermore, we use the number of bit change rate (NBCR) to quantitatively compute the difference between encrypted and decrypted images. NBCR can be described as

$$NBCR = \frac{H[Q_1, Q_2]}{L} \times 100\%,$$

where L represents the length of Q_1, Q_2 , and $H[Q_1, Q_2]$ represents the Hamming distance [3]. If S_1 and S_2 are two independent sequences, the ideal NBCR is close to 50%. Next, we provide two group slightly keys to encrypt and decrypt the plain image and cipher image, respectively. The NBCR results are calculated in Table 6 and Table 7. In Table 6 and Table 7, if a slightly change appeared in key, then it will lead to totally different encrypted and decrypted results. So, the SPCCS-based encryption algorithm is quite sensitive to key.

Fig. 13 Key sensitivity analysis in encryption process: (a) plain-image P ; (b) the cipher-image C_1 with $x_0 = 0.123$; (c) the cipher-image E_2 with $x_0 = 0.1230000000000001$; (d) the difference between E_1, E_2 and $|E_1 - E_2|$.

7.4 Key sensitivity analysis

Apparently, the security level of key is the most important factor of an encryption algorithm. So if there is a slightly change in the key, it must lead to totally different plain or cipher image [19]. In this subsection, we do the encryption and decryption simulation with very

7.5 Capability of defending differential attack

Except for the key sensitivity, the SPCCS-based algorithm must be sensitive to the slightly change in

Fig. 14 Key sensitivity analysis in decryption process. (a) the cipher-image E_1 with $x_0 = 0.123$; (b) the decrypted result with $x_0 = 0.123$; (c) the decrypted result E_2 with $x_0 = 0.1230000000000001$; (d) the difference between E_1 , E_2 and $|E_1 - E_2|$.

Table 6 The NBCR of two encrypted images

Image	Ours	[42]	[39]	[2]
Lena	50.03%	50.01%	50.00%	50.01%
baboon	50.00%	49.95%	49.96%	49.98%
peppers	49.96%	50.02%	49.97%	49.99%
boat.512	49.99%	49.97%	49.99%	49.97%

Table 7 The NBCR of two decrypted images

Image	Ours	[42]	[39]	[2]
Lena	49.98%	50.01%	49.99%	49.98%
baboon	50.03%	49.97%	50.00%	49.96%
peppers	50.03%	49.98%	49.98%	49.99%
boat.512	49.95%	50.03%	50.00%	49.99%

the plain image. The number of pixels change rate (NPCR) and unified average changing intensity (UACI) are two crucial indicators to evaluate this sensitivity. The detailed definition of NPCR and UACI are shown by

$$\begin{cases} NPCR = \sum_{i,j} \frac{I(i,j)}{G}, \\ UACI = \frac{1}{G} \sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{L}, \end{cases}$$

where

$$I(i,j) = \begin{cases} 0, & E_1(i,j) \neq E_2(i,j), \\ 1, & E_1(i,j) = E_2(i,j). \end{cases}$$

Note that G is the total number of pixels of encrypted image, and L is the gray level of the image. Recently, the expected scores of NPCR and UACI were shown in [10], which are given by

$$\begin{cases} NPCR_e = (1 - \frac{1}{2^{\log \frac{L}{2}}}) \times 100\%, \\ UACI_e = \frac{1}{L^2(L-1)} \sum_{i=1}^{L-1} i(i+1) \times 100\%. \end{cases}$$

If $L=256$, then $NPCR_e = 99.6094\%$ and $UACI_e = 33.4635\%$. It means that if the NPCR and UACI value of cipher image are close to 99.6094% and 33.4635%, the cipher image will have stronger ability to resist differential attack. The results are shown in Table 8 and Table 9, respectively. In Table 8 and Table 9, the NPCR

Table 8 $NPCR_e$ performance

Image	Ours	[42]	[39]	[2]
Lena	99.6048%	99.6117%	99.4171%	99.6143%
difference	-0.0046%	-0.0023%	0.1923%	-0.0049%

Table 9 $UACI_e$ performance

Image	Ours	[42]	[39]	[2]
Lena	33.4566%	33.4356%	33.3465%	33.4527%
difference	0.0069%	0.0279%	0.117%	0.0108%

and UACI of SPCCS-based algorithm has the smallest difference to the ideal value than that of Refs. [2, 39, 42]. Thus, the proposed SPCCS-based scheme is very sensitive to slightly modification in plain image.

7.6 Ability of resisting chosen-plaintext and chosen-ciphertext attacks

Chosen-plaintext and chosen-ciphertext attacks are widely used for attacking in cryptanalysis. For the SPCCS-based encryption algorithm, specific operations can be used to resist chosen-plaintext and chosen-ciphertext attacks:

- The size of plain image is changed by pixel segmentation operation, and chaotic sequences are used to control the pixel value after segmentation. Then, the pixel value of the plain image is segmented for several times. Even if an attacker uses a chosen-plaintext and chosen-ciphertext attacks, it is difficult to obtain the complete pixel value information from the cipher image.
- In the pixel diffusion operation, there is an operation to accumulate pixel values, which affects the subsequent diffusion process. Furthermore, the block chaotic matrix confusion operation disturbs the distribution of pixel values in a plain image. After two rounds confusion and diffusion operations, each pixel value information of plain image is expanded to the whole cipher image. Therefore, slight changes in the plain images can result in huge differences in cipher images.

- The pixel segmentation operation makes the size of the cipher image different from the size of the corresponding plain image, and links the size of the cipher image and the plain image.

7.7 Data loss attack analysis

The noise and data loss can influence digital images during transmission through the network and storage in physical media. An image encryption algorithm should resist these abnormal phenomena. Then, we provide some experiments on data loss and noise analyses. Observing Fig. 15, the SPCCS-based algorithm can decode the experimental cipher images with a good visual effect by 3%, 10%, 30% data loss, respectively. Moreover, even the encrypted image is added Salt & Pepper noise, the SPCCS-based algorithm also can decrypt the cipher images with a good visual effect, which can be seen in Fig. 16.

Fig. 15 Results on data loss attack: (a) 3%, 10%, 30% data loss with a black square in cipher-image; (b) the decrypted images of (a); (c) 3%, 10%, 30% data modification with white square in cipher image; (d) the encrypted images of (c).

Fig. 16 Results on noise attack: (a) 1%, 2%, 3% Salt & Pepper noise in cipher image; (b) the decrypted images of (a).

8 Conclusion

In this paper, we proposed a one-dimensional sinusoidal polynomial composite chaotic system satisfying Devaney's definition of chaos. Its dynamics properties were analyzed comprehensively. Moreover, a new image encryption algorithm combining pixel segmentation operation and block chaotic matrix confusing operation with the chaotic system was established and analyzed by various metrics, including key size analysis, histogram analysis, correlation analysis, local Shanny entropy, key sensitivity analysis, ability of defending differential attack, ability of resisting chosen-plaintext and chosen-ciphertext attacks, and data loss attack. This work will promote application of cascading multiple chaotic system in protecting image data communication.

Acknowledgements This study was funded by the Natural Science Foundation of Liaoning Province (NO. 2020-MS-080); National Key Research and Development Program of China (No. 2017YFF0108800).

Data availability statements The datasets analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Ashish, Cao, J., Chugh, R.: Chaotic behavior of logistic map in superior orbit and an improved chaos-based traf-

- fic control model. *Nonlinear Dynamics* **94**(2), 959–975 (2018)
2. Bao, L., Yi, S., Zhou, Y.: Combination of sharing matrix and image encryption for lossless (k, n) -secret image sharing. *IEEE Transactions on Image Processing* **26**(12), 5618–5631 (2017)
3. Castro, J.C.H., Sierra, J.M., Sez nec, A., Izquierdo, A., Ribagorda, A.: The strict avalanche criterion randomness test. *Mathematics and Computers in Simulation* **68**(1), 1–7 (2005)
4. Chai, X., Fu, X., Gan, Z., Lu, Y., Chen, Y.: A color image cryptosystem based on dynamic dna encryption and chaos. *Signal Processing* **155**, 44–62 (2019)
5. Devaney, R.L.: An introduction to chaotic dynamical systems. Westview Press (1986)
6. Fütter, B., Avrutin, V., Schanz, M.: The discontinuous flat top tent map and the nested period incrementing bifurcation structure. *Chaos, Solitons & Fractals* **45**(4), 465–482 (2012)
7. Ge, X., Lu, B., Liu, F., Luo, X.: Cryptanalyzing an image encryption algorithm with compound chaotic stream cipher based on perturbation. *Nonlinear Dynamics* **90**(2), 1141–1150 (2017)
8. Guesmi, R., Farah, M.A.B., Kachouri, A., Samet, M.: A novel chaos-based image encryption using dna sequence operation and secure hash algorithm sha-2. *Nonlinear Dynamics* **83**(3), 1123–1136 (2016)
9. Hu, T., Liu, Y., Gong, L.H., Ouyang, C.J.: An image encryption scheme combining chaos with cycle operation for dna sequences. *Nonlinear Dynamics* **87**(1), 51–66 (2017)
10. Hua, Z., Jin, F., Xu, B., Huang, H.: 2d logistic-sine-coupling map for image encryption. *Signal Processing* **149**, 148–161 (2018)
11. Hua, Z., Zhou, B., Zhou, Y.: Sine-transform-based chaotic system with fpga implementation. *IEEE Transactions on Industrial Electronics* **65**(3), 2557–2566 (2018)
12. Hua, Z., Zhou, B., Zhou, Y.: Sine chaotification model for enhancing chaos and its hardware implementation. *IEEE Transactions on Industrial Electronics* **66**(2), 1273–1284 (2019)
13. Hua, Z., Zhou, Y.: Dynamic parameter-control chaotic system. *IEEE Transactions on Cybernetics* **46**(12), 3330–3341 (2015)
14. Hua, Z., Zhou, Y.: One-dimensional nonlinear model for producing chaos. *IEEE Transactions on Circuits and Systems I: Regular Papers* **65**(1), 235–246 (2017)
15. Korabel, N., Klages, R.: Fractality of deterministic diffusion in the nonhyperbolic climbing sine map. *Physica D: Nonlinear Phenomena* **187**(1–4), 66–88 (2004)
16. Lan, R., He, J., Wang, S., Gu, T., Luo, X.: Integrated chaotic systems for image encryption. *Signal Processing* **147**, 133–145 (2018)
17. Li, B., Liao, X., Jiang, Y.: A novel image encryption scheme based on improved random number generator and its implementation. *Nonlinear Dynamics* **95**, 1781–1805 (2019)
18. Li, C., Feng, B., Li, S., Kurths, J., Chen, G.: Dynamic analysis of digital chaotic maps via state-mapping networks. *IEEE Transactions on Circuits and Systems I: Regular Papers* **66**(6), 2322–2335 (2019). doi:10.1109/TCSI.2018.2888688
19. Li, C., Lin, D., Lü, J., Hao, F.: Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE Multimedia* **25**(4), 46–56 (2018). doi:10.1109/MMUL.2018.2873472
20. Li, C., Tan, K., Feng, B., Lü, J.: The graph structure of the generalized discrete arnold cat map. *IEEE Transactions on Computers* (2021). doi:10.1109/TC.2021.3051387
21. Li, C., Zhang, Y., Xie, E.Y.: When an attacker meets a cipher-image in 2018: A Year in Review. *Journal of Information Security and Applications* **48**, art. no. 102,361 (2019). doi:10.1016/j.jisa.2019.102361
22. Li, T.Y., Yorke, J.A.: Period three implies chaos. *The American Mathematical Monthly* **82**(10), 985–992 (1975). doi:10.2307/2318254
23. Liu, L., Huang, H., Hu, S.: Lorenz chaotic system-based carbon nanotube physical unclonable functions. *IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems* **37**(7), 1408–1421 (2018). doi:10.1109/TCAD.2017.2762919
24. Lorenz, E.N.: Deterministic nonperiodic flow. *Journal of The Atmospheric Sciences* **20**(2), 130–141 (1963)
25. Luo, L., Hou, B.: Li-yorke chaos for invertible mappings on compact metric spaces. *Archiv Der Mathematik* **108**(1), 65–69 (2017)
26. Ma, Y., Li, C., Ou, B.: Cryptanalysis of an image block encryption algorithm based on chaotic maps. *Journal of Information Security and Applications* **54**, art. no. 102,566 (2020). doi:10.1016/j.jisa.2020.102566
27. Pak, C., Huang, L.: A new color image encryption using combination of the 1d chaotic map. *Signal Processing* **138**, 129–137 (2017)
28. Peng, Y., He, S., Sun, K.: A higher dimensional chaotic map with discrete memristor. *Aeu—international Journal of Electronics and Communications* **129**, art. no. 153,539 (2021). doi:10.1016/j.aee.2020.153539
29. Wang, Q., Yu, S., Guyeux, C., Bahi, J.M., Fang, X.: Theoretical design and circuit implementation of integer domain chaotic systems. *International Journal of Bifurcation and Chaos* **24**(10), 1450,128 (2014)
30. Wang, Q., Yu, S., Li, C., Lü, J., Fang, X., Guyeux, C., Bahi, J.: Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. *IEEE Transactions on Circuits and Systems I: Regular Papers* **63**(3), 401–412 (2016). doi:10.1109/TCSI.2016.2515398
31. Wang, X., Feng, L., Li, R., Zhang, F.: A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. *Nonlinear Dynamics* **95**(4), 2797–2824 (2019)
32. Wiggers, V., Rech, P.C.: Chaos, periodicity, and quasiperiodicity in a radio-physical oscillator. *International Journal of Bifurcation and Chaos* **27**(07), 1730,023 (2017)
33. Wu, J., Liao, X., Yang, B.: Image encryption using 2d hénon-sine map and dna approach. *Signal Processing* **153**, 11–23 (2018)
34. Wu, X., Zhu, P.: Li-yorke chaos in a coupled lattice system related with belusov-zhabotinskii reaction. *Journal of Mathematical Chemistry* **50**(5), 1304–1308 (2012)
35. Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J.P., Natarajan, P.: Local shannon entropy measure with statistical tests for image randomness. *Information Sciences* **222**, 323–342 (2013)
36. Xie, E.Y., Li, C., Yu, S., Lü, J.: On the cryptanalysis of Fridrich’s chaotic image encryption scheme. *Signal Processing* **132**, 150–154 (2017). doi:10.1016/j.sigpro.2016.10.002
37. Ye, G., Pan, C., Huang, X., Mei, Q.: Correction to: an efficient pixel-level chaotic image encryption algorithm. *Nonlinear Dynamics* **94**(4), 3155–3155 (2018)
38. Zheng, J., Hu, H., Xia, X.: Applications of symbolic dynamics in counteracting the dynamical degradation

- of digital chaos. *Nonlinear Dynamics* **94**(2), 1535–1546 (2018)
39. Zhou, Y., Bao, L., Chen, C.P.: A new 1d chaotic system for image encryption. *Signal Processing* **97**, 172–182 (2014)
40. Zhou, Y., Hua, Z., Pun, C.M., Chen, C.L.P.: Cascade chaotic system with applications. *IEEE Transactions on Cybernetics* **45**(9), 2001–2012 (2015)
41. Zhu, C.: A novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications* **285**(1), 29–37 (2012)
42. Zhu, H., Zhang, X., Yu, H., Zhao, C., Zhu, Z.: An image encryption algorithm based on compound homogeneous hyper-chaotic system. *Nonlinear Dynamics* **89**(1), 61–79 (2017)