



Constructive approach and randomization of a two-parameter chaos system for securing data

Olalekan Taofeek Wahab , Salaudeen Alaro Musa , AbdulAzeez Kayode Jimoh , Kazeem Adesina Dauda 

Department of Mathematics and Statistics, Kwara State University, Malete, Nigeria

Abstract

Secure communication techniques are important due to the increase in the number of technology users across the world. Likewise, a more random encryption algorithm suitable to secure data from unauthorised users is highly expected. This paper proposes a two-parameter nonlinear chaos map that is sensitive to the trio seed (s_0, α, λ) and has better information encryption. We introduce the parameter α to linearise the conventional chaos system, which in turn brings a delay in the cryptosystems. The delay is a phenomenon that changes the chaotic features of a system. A small delay in the system leads to more aperiodicity and the unpredictability of the chaotic attractions. We normalise the new chaos map and use the Lipschitz and pseudo-contractive operators to obtain its irregularity region in Hilbert spaces. We also analyse the chaos map in terms of trajectory, Lyapunov exponent, complexity, and information entropy. Results obtained show that the new chaos map has a wide chaotic range and better statistical properties. It also maintains low complexity due to its linearity and produces more key spaces than most existing chaotic maps.

DOI:10.46481/jnsps.2024.1747

Keywords: Two-parameter chaos system, Cryptosystems, Encryption algorithm, Lipschitz map, Pseudo-contractive operator

Article History :

Received: 27 August 2023

Received in revised form: 10 April 2024

Accepted for publication: 25 April 2024

Published: 21 May 2024

© 2024 The Author(s). Published by the [Nigerian Society of Physical Sciences](#) under the terms of the [Creative Commons Attribution 4.0 International license](#). Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

Communicated by: T. Latunde

1. Introduction

Nonlinear dynamical system is the study of physical (chaos) phenomena that are unsteady or irregular in nature. The chaos phenomenon is the study of nonlinear systems that are sensitive to parameter seeds. Due to the rapid development of communication technologies and the wide use of internet networks, there is a need for proper protection of vital information such as personal messages, business messages, payment platforms, etc. In communication science, the primary reference source for data


protection is cryptology [1]. The most widely used chaos map in cryptosystems is the one-dimensional logistic map which was popularized by Robert May in 1976, a biologist, and written down by Pierre Fracois Verhulst. The logistic map is a non-linear discrete function that is simple to implement in an encryption algorithm, and it is given by

$$x_{i+1} = \mu x_i(1 - x_i), \quad (1)$$

where $\mu \in (0, 4]$ is a control parameter and $x \in [0, 1]$ is called the state value. Many encryption algorithms have been proposed from the logistic map to secure data through random bit sequences in cryptanalysis. In 1998, a method of designing pseudo random number generators (PRNG) based on the logistic map was proposed in Ref. [2]. Other constructions of

*Corresponding author: Tel.: +234-803-522-4754.

Email address: taofeek.wahab@kwasu.edu.ng (Olalekan Taofeek

Wahab )

PRNG model based on chaotic logistic maps of one to three dimensions are proposed in Refs. [3–10]. In Ref. [11], Li et al. introduced a PRNG based on the spatiotemporal chaos-based map through an unidirectional coupling map lattice composed of logical maps for the construction. Many contributions in chaos-based hardware implementation of PRNGs such as fully digital circuits, Field Programmable Gate Arrays (FPGAs) can be seen in Refs. [12–14]. For various evaluation of chaos-based systems using statistical test tools, see Refs. [1, 15, 16]. Notably in Ref. [9], the two-dimensional logistic chaotic map was proposed to cryptanalyse image encryption. It is given by

$$\begin{aligned} x_{i+1} &= r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} &= r(3x_{i+1} + 1)y_i(1 - y_i), \end{aligned} \quad (2)$$

where $r \in (-1, \infty)$ is the system parameter with concentration on the interval $r \in [1.1, 1.19]$ and $(x_i; y_i)$ is the pair-wise state point at the i -th iteration. The algorithm (2) was cryptalysed using diffusion, permutation, and transposition properties. The delay linear coupling logistic map (DLCL) was introduced in Ref. [17] with the structure defined by:

$$x_{i+1} = F(x_i + ax_{i+1}), \quad (3)$$

where F is given by the logistic map (1) and $a \in (0, 1)$. The diffusion and good encryption effects are achieved for the DLCL, and the encryption efficiency of the algorithm is improved. Recently in Ref. [15], the enhanced digital logistic map

$$x_{i+1} = 4x_i(1 - x_i) + dx_i(x_i - 1), \quad (4)$$

where $d \in [0, 0.430054328)$, was introduced in order to optimise the logistic map (1) by using the perturbation operator $\mu = 4 - d$ which reduces the degradation of digital chaos. The hardware implementation of this digital chaos was carried out with the aid of stochastic computing.

This paper, however, suggests a two-parameter logistic map that is independent of the above mentioned chaotic maps and is highly sensitive to the trio seed (s_0, α, λ) . It enhances degradation of the chaos system and produces a more robust and efficient encryption algorithm. Also, it has a relatively flexible structure in which a slight change in one of its parameters disturbs the trajectory to extend periodicity and, in turn, produce a very large key space with good entropy and information criteria.

2. The two-parameter chaos system

Consider a real-valued nonlinear function $g : \mathbb{R} \rightarrow \mathbb{R}$. To find some unique points $p \in \mathbb{R}$ for which

$$g(p) = 0,$$

we seek a rule $f : \mathbb{R} \rightarrow \mathbb{R}$ such that

$$f(p) = p - g(p). \quad (5)$$

Some notes on the mapping f are presented as follows:

- The point p is a fixed point of f if $f(p) = p$.

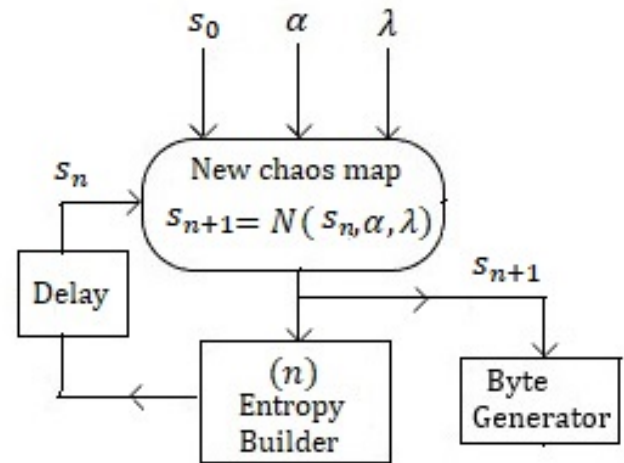


Figure 1. Block diagram of the new chaos map.

- The point p is a periodic point of period n if $f^n(p) = p$.
- The point p is an eventually periodic point of period n if there exists $k > 0$ such that $f^{n+i}(p) = f^i(p)$ for all $i \geq k$.
- A point s is called a critical point if $f'(s) = 0$. A critical point is non-degenerate if $f''(s) \neq 0$ and degenerate if $f''(s) = 0$.
- The sets of points $\{s, f(s), f^2(s), \dots\}$, $\{s, f^{-1}(s), f^{-2}(s), \dots\}$ are called the forward and backward orbits of s , respectively.
- If f is a homeomorphism, the full orbit of s is the set of points $f^m(s)$ for $m \in \mathbb{Z}$.

Now, let f and g be related as given in the map (5). Let $s_0 \in \mathbb{R}$ be fixed and let $s_1 = s_0 + v_0$ be a cluster around s_0 . Set $s_1 = f(s_0)$, the linearisation of f is the approximant:

$$s_1 \approx s_0 + \alpha v_0 + O(v_0^2),$$

where $\alpha > 0$ is a weight multiplier associated with f . Inductively, there gives

$$s_{n+1} = s_n + \alpha v_n, \quad n = 0, 1, 2, \dots, \quad (6)$$

where $v_n = f(s_n) - s_n$. Let $h : \mathbb{R} \rightarrow \mathbb{R}$ be an update of f , then the equivalent form of system (6) is given by

$$s_{n+1} = h(s_n) = N(s_n, \alpha, \lambda), \quad (7)$$

where $N(s_n, \alpha, \lambda) \equiv s_n - \alpha(s_n - f(s_n))$ and f is defined by the chaos map (1). This will be referred to as a one-dimensional two-parameter chaos map. Obviously, the system (6) is the chaos map (1) with $\alpha = 1$. Also, it is easy to see that there is no stride if $\alpha = 0$. In the sequel, there will be special emphasis on some choices of $\alpha > 0$. Figure 1 describes the new chaos map.

2.1. Normalisation

Here, the chaos map (7) is restricted to a non-wandering subset of \mathbb{R} . To begin with, we present the following theorem.

Theorem 1. Let $h : \mathbb{R} \rightarrow \mathbb{R}$ be a function given by (7), then the critical value of h is the coordinate (s_0, h_0) , where

$$h_0 = s_0 - \alpha(s_0 - \lambda s_0(1 - s_0)) \text{ and } s_0 = \frac{1}{2} + \frac{1 - \alpha}{2\alpha\lambda},$$

for $\alpha, \lambda \in (0, \infty)$.

Proof:

Consider the chaos map (7),

$$h(s) = s - \alpha(s + \lambda s(s - 1)), \quad s \in \mathbb{R}.$$

Observe that h is quadratic in s and so

$$h'(s) = 1 - \alpha(1 + \lambda(2s - 1)).$$

At the critical point $s_0 \in \mathbb{R}^+$, where $h'(s_0) = 0$, there gives

$$s_0 = \frac{1}{2} \left(1 + \frac{1 - \alpha}{\alpha\lambda} \right), \text{ for any } \alpha > 0, \lambda \in (0, \infty).$$

Substituting s_0 into h yields the desired result.

Remark 2. i. If $\alpha < 1$ and λ grows without bound, then $s_0 \rightarrow \frac{1}{2}^+$.

ii. If $\alpha > 1$ and λ grows without bound, then $s_0 \rightarrow \frac{1}{2}^-$.

iii. If $\alpha = 1$ and for any $\lambda \in \mathbb{R}^+$, then $s_0 = \frac{1}{2}$.

In Remark 2(iii.), h has its maximum at $s_0 = \frac{1}{2}$ for which $h_0 = \frac{1}{4}$. In this case, h is restricted in $[0, 1] \subset \mathbb{R}$ for $\lambda \in (0, 4]$. If otherwise, all points of h become wandering for $\lambda > 4$. In order that the Remark 2(i.) and (ii.) follow suit, we present the following theorem:

Theorem 3. Assume that h is restricted in the interval $[0, 1] \subset \mathbb{R}$ and has critical value at $s_0 \in [0, 1]$, then the system parameter λ is given by

$$\lambda = \begin{cases} 1 + \frac{1}{\alpha} - 2\alpha^{-\frac{1}{2}}, & \text{for } \alpha > 0, \alpha \neq 1, \\ 1 + \frac{1}{\alpha} + 2\alpha^{-\frac{1}{2}}, & \text{for } \alpha > 0, \alpha \neq 1, \\ \{0, 4\}, & \text{for } \alpha = 1. \end{cases}$$

Proof: Let $h : [0, 1] \rightarrow [0, 1]$ be given by map (7) and satisfies the hypothesis of Theorem 1. Since h does not exceed 1 and $s_0 = \frac{1}{2} \left(1 + \frac{1 - \alpha}{\alpha\lambda} \right)$, then

$$(1 - \alpha) \left(\frac{1}{2} + \frac{1 - \alpha}{2\alpha\lambda} \right) + \alpha\lambda \left(\frac{1}{2} + \frac{1 - \alpha}{2\alpha\lambda} \right) \left(1 - \left(\frac{1}{2} + \frac{1 - \alpha}{2\alpha\lambda} \right) \right) = 1.$$

This is further reduced to the form

$$\alpha^2 \lambda^2 - 2(\alpha^2 + \alpha)\lambda + (1 - \alpha)^2 = 0.$$

Table 1. Relationship between α , λ_1 and λ_2 .

	α	λ 's	Monotonic shifts	
λ_1	$(0, 1)$	$(0, \infty)$	decreasing	Non-monotonic for all α
	$\alpha = 1$	$\lambda_1 = 0$	critical	
λ_2	$(1, \infty)$	$(0, 1)$	increasing	
	$(0, 1)$	$(4, \infty)$	decreasing	Monotonic for all α
	$\alpha = 1$	$\lambda_2 = 4$	critical	
	$(1, \infty)$	$(1, 4)$	decreasing	

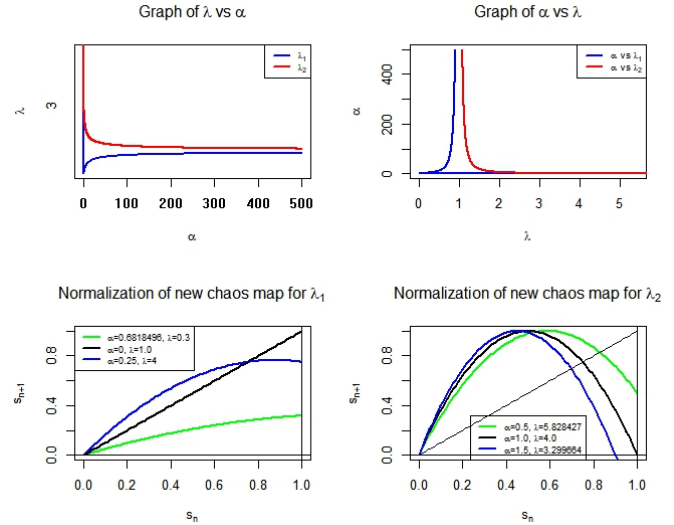


Figure 2. Normalization of new chaos map.

By completing the square in the parameter λ , we have

$$\lambda_1 = 1 + \frac{1}{\alpha} - 2\alpha^{-\frac{1}{2}} \text{ and } \lambda_2 = 1 + \frac{1}{\alpha} + 2\alpha^{-\frac{1}{2}}. \quad (8)$$

If $\alpha = 1$ in equation (8), then $\lambda_1 = 0$ and $\lambda_2 = 4$. As required. Summarily, we present the relationship between parameters α , λ_1 and λ_2 in Table 1 and Figure 2. In Figure 2 (top), the parameter λ_1 decreases when $\alpha \in (0, 1)$ and increases for $\alpha \in (1, \infty)$, and thus, attains its minimum := 0 at $\alpha = 1$. On the other hand, λ_2 decreases throughout for all $\alpha \in (0, \infty)$. Moreover, both the curves of λ_1 and λ_2 are asymptotic (approach 1) as α approaches the large value. Also, the graphs of s_{n+1} vs s_n for various λ_1 and λ_2 are plotted. Three cases are considered for each λ_1 and λ_2 in Figure 2 (bottom). We observe that the curve of new chaos map (7) is becoming linear when α decreases in $[0, 1)$ wherein the curve h lies outside the interval $[0, 1]$; and is becoming nonlinear when α increases in $[1, \infty)$ wherein $h \in [0, 1]$.

2.2. Chaotic and non-chaotic attractive regions

To buttress the normality supposition in the immediate subsection, we study the geometric properties of the new chaos map using the Lipschitz and pseudocontractive operators to classify the orbits that are chaotic attractive and non-attractive, periodic and aperiodic, predictable and unpredictable, and so on. The following definitions are versions of those that are evident in Refs. [18, 19].

Definition 4. Let $(X, \|\cdot\|)$ be a non-empty normed space and $f : X \rightarrow X$ be a self-map. The map f is called a δ -Lipschitz map for $\delta > 0$ if

$$\|f(s) - f(t)\| \leq \delta \|s - t\|, \forall s, t \in X. \tag{9}$$

It is said to be δ -contractive if $\delta \in (0, 1)$.

Definition 5. Let \mathbb{H} be a Hilbert space with norm $\|\cdot\|$ and inner product $\langle \cdot, \cdot \rangle$. An operator $f : \mathbb{H} \rightarrow \mathbb{H}$ is said to be a generalized pseudocontractive map if there exists a constant $r > 0$ such that

$$\langle f(s) - f(t), s - t \rangle \leq r \|s - t\|^2, \forall s, t \in \mathbb{H}. \tag{10}$$

Lemma 6. Let $f : [0, 1] \rightarrow [0, 1]$ be given by the logistic map (1). Then, f satisfies the Lipschitz condition (9) and its system parameter $\lambda = \delta$.

Proof: Let $s, t \in [0, 1]$ and $f : [0, 1] \rightarrow [0, 1]$ be the logistic map (1), then

$$\begin{aligned} \|f(s) - f(t)\|_\infty &= \|\lambda s(1-s) - \lambda t(1-t)\|_\infty \\ &= \|\lambda(s-t) - (s^2 - t^2)\|_\infty \\ &= \|\lambda[1 - (s+t)](s-t)\|_\infty \\ &\leq \lambda \|1 - s - t\|_\infty \|s - t\|_\infty \\ &= \lambda \sup\{1 - s - t\} \|s - t\|_\infty = \lambda \|s - t\|_\infty. \end{aligned}$$

Letting $\delta = \lambda$ gives the desired result.

Lemma 7. Let $(X, \|\cdot\|)$ be a Banach space and let $f : X \rightarrow X$ be a map satisfying δ -contractive condition

$$\|f(s) - f(t)\| \leq \delta \|s - t\|, \forall s, t \in X. \tag{11}$$

Then, f has an attractive (non-chaotic) unique fixed point.

The proof of Lemma 7 follows the contraction mapping principle. By virtue of Lemma 7, if $\delta \geq 1$, f has a repelling (chaotic) fixed point.

Theorem 8. Let K be a non-empty closed convex subset of a real Hilbert space \mathbb{H} and let $f : K \rightarrow K$ be a Lipschitz operator (9) and generalized pseudo-contractive condition (10) with $\delta, r > 0$. Then,

- I. the new chaos map h has an attractive unique fixed point;
- II. For $s_0 \in K$, the new chaos sequence $\{s_n\}_{n=0}^\infty$ given by

$$s_{n+1} = N(s_n, \alpha, \lambda), \quad n = 0, 1, 2, \dots, \tag{12}$$

converges (strongly) to the fixed point of f , $\forall \alpha \in (0, 1)$ satisfying

$$0 < \alpha < (1-r)/(1-2r+\lambda^2).$$

Proof:

I. Let $s, t \in K$ and let h be given by map (7). Then,

$$\begin{aligned} \|h(s) - h(t)\|^2 &= \|(1-\alpha)s + \alpha f(s) - (1-\alpha)t - \alpha f(t)\|^2 \\ &= \|(1-\alpha)(s-t) + \alpha(f(s) - f(t))\|^2 \end{aligned}$$

$$\begin{aligned} &\leq (1-\alpha)^2 \|s-t\|^2 + 2\alpha(1-\alpha) \langle f(s) - f(t), s-t \rangle \\ &\quad + \alpha^2 \|f(s) - f(t)\|^2 \end{aligned}$$

Lemma 6, conditions (9) and (10) imply that

$$\begin{aligned} \|h(s) - h(t)\|^2 &\leq (1-\alpha)^2 \|s-t\|^2 + 2\alpha(1-\alpha)r \|s-t\|^2 \\ &\quad + \alpha^2 \lambda^2 \|s-t\|^2 \\ &= [(1-\alpha)^2 + 2\alpha(1-\alpha)r + \alpha^2 \lambda^2] \|s-t\|^2 \end{aligned}$$

Let $\theta^2(\alpha, \lambda, r) = (1-\alpha)^2 + 2\alpha(1-\alpha)r + \alpha^2 \lambda^2$, we obtain

$$\|h(s) - h(t)\| \leq \theta \|s - t\| \tag{13}$$

Now, by optimising θ with respect to the parameter α gives

$$\theta_\alpha = (\lambda^2 - 2r + 1)\alpha - (1-r)$$

So for $\theta_\alpha = 0$, we obtain

$$\alpha = \frac{1-r}{1-2r+\lambda^2} \tag{14}$$

This resulted to the following cases:

- i. if $r = \lambda$, then $\alpha = \frac{1}{1-\lambda}$, $\lambda \neq 1$, implies that $\theta = 0$.
- ii. if $r < \lambda$, then $1-r < 1-2r+\lambda^2$ (that is, $\alpha < 1$) implies that $\theta < 1$. Hence, the conclusion follows from the hypothesis of Lemma 7.

II. This follows from inequality (13) for $\theta < 1$.

Remark 9. Observe that if $r > \lambda$, then $1-r > 1-2r+\lambda^2$ (that is, $\alpha > 1$) implies that $\theta > 1$. In this case, h has a repelling fixed point where chaotic attractions set in. Also, the choice of $\alpha > 1$ changes the chaotic attractor's interval from $\lambda \in (3.569945672, 4]$ to $\lambda \in (1, 4]$, see Table 1.

2.3. Periodic doubling

This subsection showcases some bifurcation diagrams of the new chaos map with respect to the two-parameter system. The bifurcation is a periodic doubling that describes the distribution of the chaotic state of the map. The sequence values associated to the chaos map is plotted against the parameter λ while α is held fixed, and with respect to α while fixing λ . In Figure 3, all choices of α maintain aperiodic except for $\alpha = 0.9$ that is wandering outside the normal set. A cascade of period-doublings fall out as λ approaches approximately 2.62, 3.2 and 3.57 for $\alpha = 1.5$, $\alpha = 1.1$ and $\alpha = 1$, respectively, in which the map becomes chaotic and the attraction changes gradually from a finite state to an infinite set of points. Also in Figure 4, all choices of λ maintain aperiodic except for $\lambda = 4.3$ that is wandering outside the set. It is apparent from Figures 3 and 4 that the chaotic state occurs for all choices of $\alpha \in [1, \infty)$ and $\lambda \in (1, 4]$.

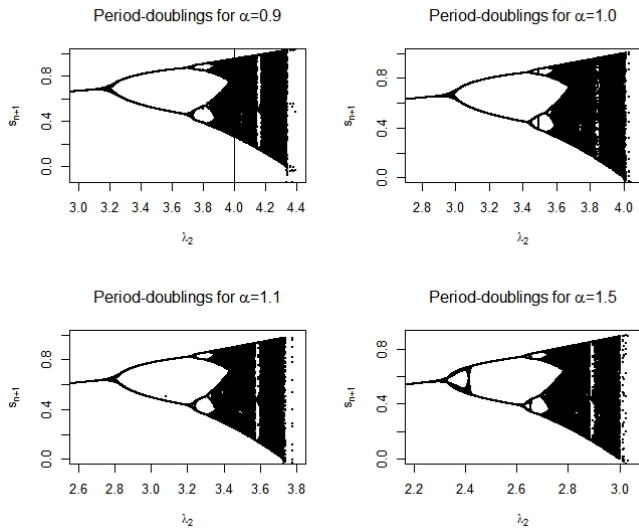


Figure 3. Period-doublings for some range of λ_2 .

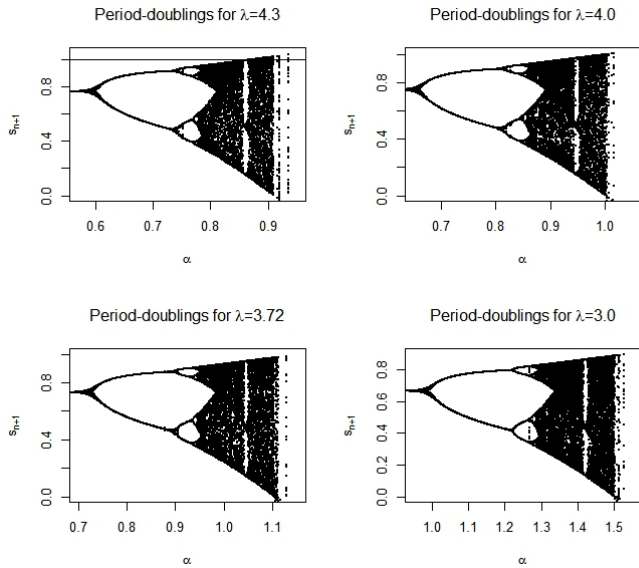


Figure 4. Period-doublings for some range of α .

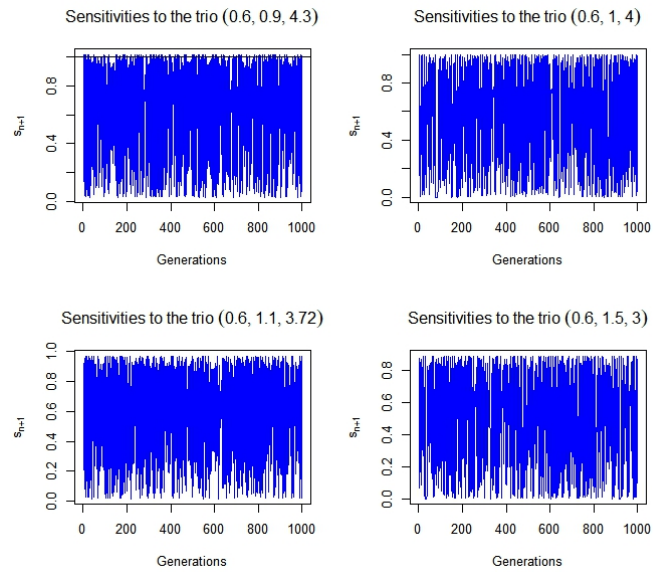


Figure 5. Sensitivities to the trio seed (s_0, α, λ) .

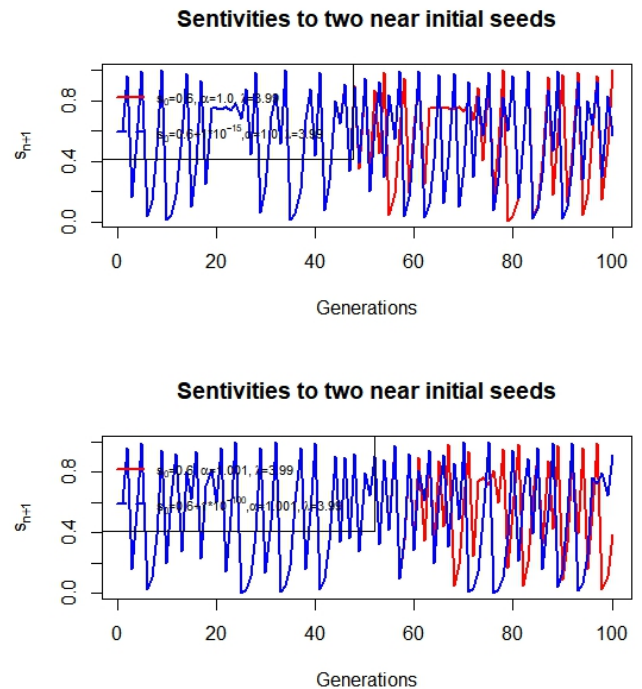


Figure 6. Sensitivities of two near orbits.

2.4. Sensitivity analysis

The sensitivities of the chaos map (7) with respect to the trio seed (s_0, α, λ) are visualised to commemorate the periodic doubling to cycles of periods in Figures 3 and 4. A small change in the initial seed yields a dramatically different results over time and likewise in the system parameters. An important feature emerges in the region $\lambda \in (1, 4]$ for various $\alpha \geq 1$ with initial seed $s_0 = 0.6$ and 1000 generations. In Figure 5, we plot the graphs for the four trios, namely, $(0.6, 0.9, 4.3)$, $(0.6, 1, 4)$, $(0.6, 1.1, 3.72)$, & $(0.6, 1.5, 3)$. All the four trios exhibit the symptoms of chaotic attractions except the trio $(0.6, 0.9, 4.3)$ [$\lambda = 4.3 > 4$] that is wandering outside the set $[0, 1]$. In Figure 6, two very near initial seeds are compared to see the key sensitivities between the trios $(0.6, 1.0, 3.99)$ and

$(0.6 + 1.0 \times 10^{-15}, 1.0, 3.99)$ for 100 generations. The two time series stay close together for about 52 generations before dispersion set in. Similar comparison is carried out for the trios $(0.6, 1.001, 3.99)$ and $(0.6 + 1.0 \times 10^{-100}, 1.001, 3.99)$ in which dispersion set in after about 60 generations. Both figures in Figure 6 illustrate symptoms of chaos, but the latter produces more keys up to about 10^{-100} while the former does not exceed 10^{-15} . In Table 2, some 8-floating point numbers are generated

Table 2. Generations of the new chaos map with trio seed (s_0, α, λ) .

Trio seed (s_0, α, λ)	Generations in million (m)	8 floating point numbers
(0.30, 1.0, 4)	1	0.5518764
(0.301, 1.2, 3.5)	1	0.0211566
(0.302, 1.5, 3.0)	1	0.0044686
(0.303, 2.0, 2.5)	2	0.5788585
(0.304, 3.0, 2.0)	2	0.6130698
(0.305, 4.0, 1.75)	2	0.2617860
(0.306, 5.0, 1.6)	3	0.4825651
(0.307, 10.0, 1.3)	3	0.0197317

with different trio seeds to show that the chaotic state remain for any value of $\alpha \in [1, \infty)$ and $\lambda \in (1, 4]$.

2.5. Lyapunov exponent

The Lyapunov exponent showcases the rate of chaotic attractions of trajectories in dynamical systems. It is usually used as an indication of positive chaos. In what follows, we obtain a Lyapunov constant τ for the new chaos map.

Let $h(s^*)$ be the new chaos map and let s^* be its fixed point such that $s^* = h(s^*)$.

Let u_n be a sequence of nearby orbits of s^* such that

$$s_n = s^* + u_n \Rightarrow s_{n+1} = h(s_n) = h(s^* + u_n).$$

By Taylor's series, we have

$$s_{n+1} \approx h(s^*) + h'(s^*)u_n + O(u_n^2).$$

This implies that

$$u_{n+1} \approx h'(s^*)u_n. \quad (15)$$

Let s_0 be an initial seed and $s_0 + u_0$ be its nearby orbit, where u_0 is exceptionally small.

Set $u_1 \approx h'(s_0)u_0$, then $u_2 \approx h'(s_1)h'(s_0)u_0$ and by induction

$$\begin{aligned} |u_n| &\approx |h'(s_{n-1})| |u_{n-1}| = \dots = |h'(s_{n-1})| |h'(s_{n-2})| \\ &\quad \times |h'(s_{n-3})| \dots |h'(s_0)| |u_0| \\ &\approx \prod_{i=0}^{n-1} |h'(s_i)| |u_0|. \end{aligned}$$

This further implies

$$\ln |u_n| \approx \sum_{i=0}^{n-1} \ln |h'(s_i)| + \ln |u_0| = \sum_{i=0}^{n-1} \ln |1 + \alpha(f'(s_i) - 1)| + \ln |u_0|.$$

Therefore,

$$|u_n| \approx |u_0| e^{n\tau},$$

where $\tau = \frac{1}{n} \sum_{i=0}^{n-1} \ln |1 + \alpha(f'(s_i) - 1)|$ is the Lyapunov exponent of the new chaos map.

- As opined in the previous section, for any $\lambda \in (0, \infty)$, the exponent τ is negative only if $\alpha < 1$. This implies that the new chaos map is stable.
- For any $\lambda \in (1, 4]$, then τ is positive only if $\alpha \geq 1$. This means that the new chaos map has some level of chaotic attractions that are wandering in the interval $[0, 1]$.
- Divergence occurs when $\lambda > 4$ and $\alpha \geq 1$.

3. Applications

For a chaos system to be suitable for cryptographic applications, it requires that the output of a random number generation (RNG) be unpredictable from earlier outputs. Thus, any sequence generated by the RNG must have the following features: (1) the output of the RNG has good statistical properties; (2) for any initial seeds, the RNG generated the sequence with no shorter periods; and (3) the correlation of successive values is poor in the sequence. In order to ensure forward unpredictability in cryptographic applications, the seed itself must be kept secret since the generation algorithm is publicly available, but for the sake of studies, initial seeds are chosen non-randomly and, in some cases, randomly. In this study, the random bit stream generator of the chaos map (6) is based on discrete choice analysis:

$$\varepsilon(x) = \begin{cases} 1; & x \geq 0.5 \\ 0; & x < 0.5. \end{cases}$$

The generator ε may be divided into substreams or blocks of random numbers. All tests are carried-out on **R** program.

3.1. Correlations

The periodic pattern in sequences can be measured through correlation. Correlation is the degree of similarity between two random variables, that is, the measure of similarities between a random variable and its shifted version. If the correlation of the sample is close to 1, it means the sequence has a better or more reliable pattern, and if it is close to zero (0), it is unreliable. This means that the map produces randomness and chaotic attractions. Here, we let the two near trios (0.2, 1.19, 3.5001) and (0.201, 1.19, 3.5001) be sample1 and sample2, respectively. In Figure 7, we plot the boxplot, histogram and scatter (nonsmooth) plots to display the mean realizations, frequency distributions, and independence of the two samples. The Pearson's product-moment correlation test of the given samples is 0.02798194 with a p -value of 0.3767, this shows the independence of each sample. We also plot the graph of autocorrelation and cross-correlation in Figure 8 to further show the independence of the two samples.

3.2. Information criterion

The Akaike information criterion (AIC) is a mathematical tool for evaluating how good a model fits the data it was obtained from. It is used to compare several possible models and determine which one is the best fit for some given data. The AIC formula is given by

$$AIC = 2K - 2\ln(L), \quad (16)$$

where K is the number of independent variables used and L is the log-likelihood estimate. Here, the default $K (= 2)$ is used. Another model selection among a finite set of models is the Schwarz-Bayesian information criterion (S-BIC or BIC). It is based on the likelihood function, and it is closely related to the AIC. A model with a low AIC (or BIC) is the best model [20, 21]. The actual difference between the two criteria is that

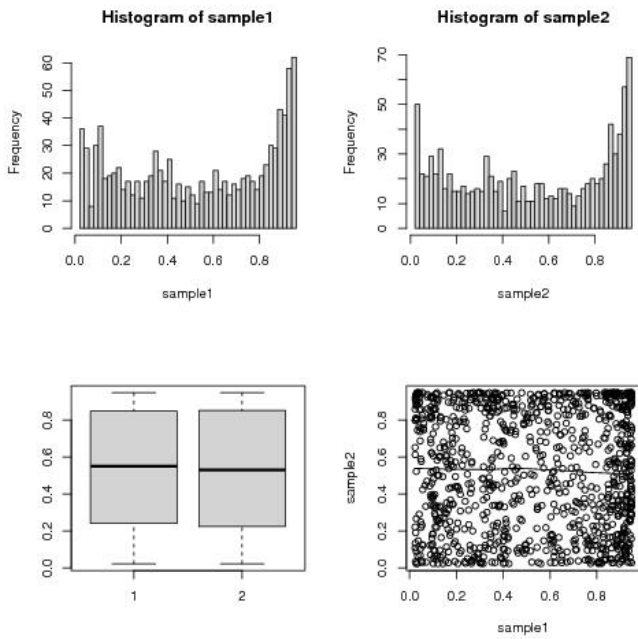


Figure 7. Boxplot and histogram of the two samples.

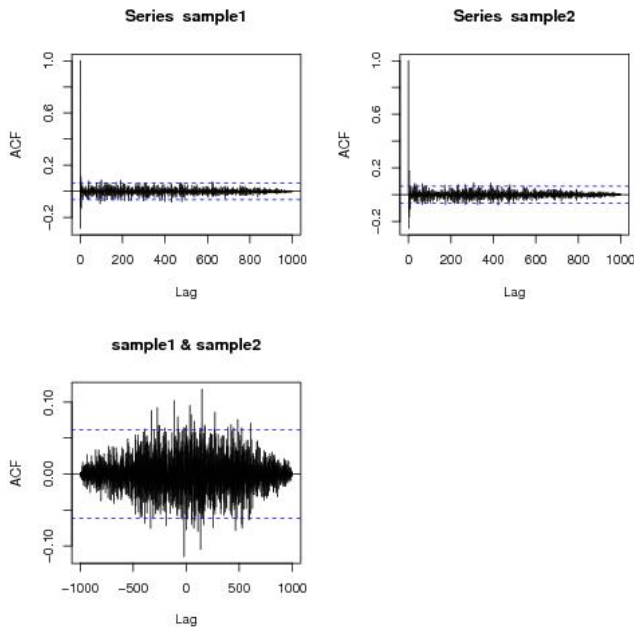


Figure 8. Auto-correlation and cross-correlation of the two samples.

the BIC penalizes a given model more for its complexity than the AIC. The following set of selections shows comparisons of models for the data generated by chaotic maps (1), (2), (3) and (6).

Model selection based on AICc and BIC for the new chaos map:

	K	AICc	BIC	Delta	Wt	Cum.Wt	LL
(0.2,1.5,2.33)	3	354.53	369.23	0.00	0.65	0.65	-174.26
(0.2,1.2,2.67)	3	356.82	371.52	2.29	0.21	0.86	-175.40
(0.2,1.1,3.0)	3	358.97	373.66	4.43	0.07	0.93	-176.47
(0.2,1.0,3.68)	3	358.99	373.69	4.46	0.07	1.00	-176.48

Model selection based on AICc and BIC for various chaos maps:

	K	AICc	BIC	Delta	Wt	Cum.Wt	LL
New chaos map	3	355.22	369.92	0.00	0.63	0.63	-174.60
Enhanced logistic map	3	357.77	372.47	2.55	0.17	0.80	-175.87
2D logistic map	3	358.80	373.50	3.58	0.10	0.90	-176.39
Logistic map	3	358.97	373.67	3.75	0.10	1.00	-176.47

The AICc and BIC model selections are used to differentiate among a set of possible models describing the relationship between the new chaos map and other fewer chaos systems (with same parameter seeds) in the literature. Due to selection based on AICc and BIC, the new chaos map considerably performs better by carrying 63% of the overall cumulative model weight and 46% ahead of the next best model. Hence, the new algorithm is exceptionally suitable for encryption analyses and implementations.

3.3. Key space analysis

A good encryption algorithm is more secure in cryptosystem if its key space is at least 2^{100} so as to frustrate brute-force attacks, for example, see Refs. [22, 23]. In the proposed map (2), the key consists of the initial seed s_0 and the two-parameter system α and λ . By Remark 9, $s_0 \in (0, 1)$, $\alpha \in [1, \infty)$ and $\lambda \in (1, 4]$. By using precision of the floating-point equal to 10^{-50} , initial seed can be any point among 10^{50} possible values. Also, by letting the $\max\{\alpha\} = 1000$, then α and λ can be any point among 999×10^{50} and $(4 - 1.001) \times 10^{50}$ values, respectively. Therefore, the key space is about $2.996 \times 10^{203} \approx 2^{676} (\gg 2^{100})$, which satisfies the general requirement of resisting any attack. Therefore, a very large key space is produced in the proposed chaos map and is suitable for securing data.

3.4. Information entropy

Information entropy is a measure of the disorderliness in chaos systems. High values of entropy mean a robust RNG, whereas low values of entropy mean a weak RNG. The more chaotic a sequence, the higher the information entropy [1, 10]. The information entropy is described as follow:

Let y_1, y_2, \dots, y_n represent a list of finite positive numbers and let $y = \sum_{i=1}^n y_i$ denote their sum. The information entropy is

$$H(y) = \sum_{i=1}^{2^n-1} p(y_i) \log_2 \frac{1}{p(y_i)}, \quad (17)$$

where $p(y_i)$ indicates the probability of each i . When the distribution of sequence values is an equal probability distribution, that is, when the probability of each value between $[0, 255]$ is $1/256$, it has the maximum entropy of $\log_2 256 = 8$ -bit. In Table 3, some experimental sample points are extracted to show a few entropies of the new chaos map for randomly selected initial seeds. Due to the test results, the entropy of each component is approximately 8 (more accurately as α becomes large) which is the ideal value for an 8-bit case. Therefore, this cryptosystem performs well for resisting an entropy attack.

Table 3. Information entropy of some samples.

Entropies of randomly selected samples					
$\alpha = 1$	$\alpha = 1.1$	$\alpha = 1.5$	$\alpha = 2$	$\alpha = 3$	$\alpha = 5$
$\lambda = 3.68$	$\lambda = 3.395$	$\lambda = 1.5$	$\lambda = 1.2$	$\lambda = 1.15$	$\lambda = 1.11$
7.930096	7.916825	7.988589	7.998697	7.998687	7.998957
7.924763	7.916868	7.994550	7.999746	7.999231	8.000000
7.921137	7.918634	7.997918	7.979209	7.999839	7.999965
7.924579	7.919688	7.995788	7.999920	7.999975	7.997963
7.927595	7.916587	7.997945	7.998820	7.999941	7.996926
7.920791	7.917058	7.996177	7.977601	7.990970	7.998748

4. Conclusion

This paper has proposed a one-dimensional two-parameter system chaos map that has a relatively simple structure, good statistical properties, and high sensitivity to the trio seed (s_0, α, λ) . The new chaotic map was normalised in the interval $[0, 1]$, where we justify the effect of parameter α relative to control parameter λ . We further classified the chaotic and non-chaotic states of the map with the imposition of pseudo-contractive operator in a Hilbert space setting. The period-doublings, Lyapunov exponent, and unpredictability of the chaos system were verified for some random seeds (s_0, α, λ) . Also, we checked the cryptographic suitability of the results, and excellent performances were recorded in all the experiments using statistical tools such as boxplot, histogram, correlation, auto-correlation and cross-correlation, information entropy, AIC, and BIC analyses. Also, the key space produced is approximately 2^{676} which is capable of resisting common attacks, namely, brute-force attacks. Thus, the encryption algorithm has relatively better performance, strong, reliable, and suitable for studying cryptosystems and implementations.

Acknowledgment

We thank the referees for their comments and suggestions, which have greatly assisted us to improve this paper.

References

- [1] C. Li, D. Lin, B. Feng, J. Lu & F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy", *IEEE Access* **6** (2008) 75834. <https://doi.org/10.1109/ACCESS.2018.2883690>.
- [2] M. Andreucot, "Logistic map as a random number generator", *Int. J. Mod. Phys. B* **12** (1998) 921. <https://doi.org/10.1142/S021797929800051X>.
- [3] W. Zhao, Z. Chang, C. Ma, C. Ma & Z. Shen, "A pseudorandom number generator based on the chaotic map and quantum random walks", *Entropy* **25** (2023) 166. <https://doi.org/10.3390/e25010166>.
- [4] H. Hu, L. Liu & N. Ding, "Pseudorandom sequence generator based on the Chen chaotic system", *Comput. Phys. Commun.* **184** (2013) 765. <https://doi.org/10.1016/j.cpc.2012.11.017>.
- [5] V. Patidar, K. K. Sud & N. K. Pareek, "A pseudo random bit generator based on chaotic logistic map and its statistical testing", *Informatika* **33** (2019) 441. <https://www.informatika.si/index.php/informatika/article/view/261/258>.
- [6] J. Teh, W. Teng, A. Samsudin & J. Chen, "A post-processing method for true random number generators based on hyperchaos with applications in audio-based generators", *Frontiers of Computer Science* **14** (2020) 146405. <https://doi.org/10.1007/s11704-019-9120-2>.
- [7] X. Y. Wang & L. Yang, "Design of pseudo-random bit generator based on chaotic maps", *Int. J. Mod. Phys.* **26** (2012) 1250208. <https://doi.org/10.1142/S0217979212502086>.
- [8] Y. Wang, Z. Liu, J. Ma & H. He, "A pseudo-random number generator based on piecewise logistic map", *Nonlinear Dyn.* **83** (2016) 2373. <https://doi.org/10.1007/s11071-015-2488-0>.
- [9] Y. Wu, G. Yang, H. Jin & J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map", *Journal of Electronic Imaging* **21** (2012) 013014. <https://doi.org/10.1117/1.JEI.21.1.013014>.
- [10] L. Xu, Z. Li, J. Li & W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps", *Opt. Lasers Eng.* **78** (2016) 17. <https://doi.org/10.1016/j.optlaseng.2015.09.007>.
- [11] P. Li, Z. Li, W. A. Halang & G. Chen, "A novel multiple pseudo random bits generator based on spatiotemporal chaos", *IFAC Proc.* **38** (2005) 1085. <https://doi.org/10.3182/20050703-6-CZ-1902.00837>.
- [12] A. S. Mansingka, A. G. Radwan & K. N. Salama, "Fully digital 1-D, 2-D and 3-D multiscroll chaos as hardware pseudo random number generators", In *Proceedings of the International Midwest Symposium on Circuits and Systems (MWSCAS)*, Boise, ID, USA, 2012, pp. 1180-1183. <https://doi.org/10.1109/MWSCAS.2012.6292236>.
- [13] Y. Mao, L. Cao & W. Liu, "Design and FPGA implementation of a pseudo-random bit sequence generator using spatiotemporal chaos", In *Proceedings of the International Conference on Communications, Circuits and Systems*, Guilin, China, 2006, pp. 2114-2118. <https://doi.org/10.1109/ICCCAS.2006.284916>.
- [14] H. T. Yang, J. R. Huang & T. Y. Chang, "A chaos-based fully digital 120 MHz pseudo random number generator", In *Proceedings of the IEEE Asia-Pacific Conference on Circuits and Systems*, Tainan, Taiwan, 2004, pp. 357-360. <https://doi.org/10.1109/APCCAS.2004.1412769>.
- [15] J. Liu, Z. Liang, Y. Luo, L. Cao, S. Zhang, Y. Wang & S. Yang, "A hardware pseudo-random number generator using stochastic computing and logistic map", *Micromachines* **12** (2021) 31. <https://doi.org/10.3390/mi12010031>.
- [16] L. Wang & H. Cheng, "Pseudo-random number generator based on logistic chaotic system", *Entropy* **21** (2019) 960. <https://doi.org/10.3390/e21100960>.
- [17] S. Li, W. Ding, B. Yin, T. Zhang & Y. Ma, "A novel delay linear coupling logistics map model for color image encryption", *Entropy* **20** (2018) 463. <https://doi.org/10.3390/e20060463>.
- [18] V. Berinde, *Iterative approximation of fixed points*, (2nd ed.) Springer-Verlag, Berlin Heidelberg, 2007. <https://doi.org/10.1007/978-3-540-72234-2>.
- [19] O. T. Wahab, R. O. Olawuyi, K. Rauf & I. F. Usamot, "Convergence rate of some two-step iterative schemes in Banach spaces", *Journal of Mathematics* **2016** (2016) 9641706. <https://doi.org/10.1155/2016/9641706>.
- [20] H. Akaike, "Akaike's information criterion", In *Lovric M. (eds) International Encyclopedia of Statistical Science*, Springer, Berlin, Heidelberg, 2011. https://doi.org/10.1007/978-3-642-04898-2_110.
- [21] G. Schwarz, "Estimating the dimension of a model", *Annals of Statistics* **6** (1978) 461. <https://doi.org/10.1214/aos/1176344136>.
- [22] G. Alvarez & S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", *Int. J. Bifurc. Chaos.* **16** (2006) 2129. <https://doi.org/10.1142/S0218127406015970>.
- [23] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption", *Nonlinear Dyn.* **92** (2018) 305. <https://doi.org/10.1007/s11071-018-4056-x>.