CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.4 / No.1 / 2022 / pp.45-58
https://doi.org/10.51537/chaos.1069002

Lyapunov Exponent Enhancement in Chaotic Maps with Uniform Distribution Modulo One Transformation

Günyaz Ablay *,[1]
*Department of Electrical-Electronics Engineering, Abdullah Gül University, Kayseri, Turkey.

ABSTRACT Most of the chaotic maps are not suitable for chaos-based cryptosystems due to their narrow chaotic parameter range and lacking of strong unpredictability. This work presents a nonlinear transformation approach for Lyapunov exponent enhancement and robust chaotification in discrete-time chaotic systems for generating highly independent and uniformly distributed random chaotic sequences. The outcome of the new chaotic systems can directly be used in random number and random bit generators without any post-processing algorithms for various information technology applications. The proposed Lyapunov exponent enhancement based chaotic maps are analyzed with Lyapunov exponents, bifurcation diagrams, entropy, correlation and some other statistical tests. The results show that excellent random features can be accomplished even with one-dimensional chaotic maps with the proposed approach.

KEYWORDS
Chaos
Lyapunov exponent
Random numbers
Cryptography
Image encryption

INTRODUCTION

Chaotic maps have a wide-range application areas in many disciplines including engineering, cryptography, statistics, physics, biology, art and philosophy (El-Hameed *et al.* (2021); Benamara *et al.* (2016); Strogatz (2015); Ruelle (1997); Banerjee *et al.* (2012)). Specifically, the need for highly secure cryptosystems is always increasing because the information technologies are continuously developing and reaching more and more people everyday in various platforms (e.g., e-banking, IoT, e-purchasing, etc.). The chaos-based cryptography is a great tool to produce secure and independent random number sequences for information security. On the other hand, only few number of chaotic maps are inherently suited for data encryption since the majority of chaotic systems are not satisfying the statistically independendent and unbiased uniform distribution which are the main properties of random key generators. Many chaotic maps have a limited key space due to their narrow chaotic ranges, which causes security issues against intruders (Luo *et al.* (2020)). In addition, the chaotic random number generators must be sufficiently fast, and there should not be any collapsing effect in long turn run.

To deal with the aforementioned issues, there is a great interest in developing novel chaotic maps with highly mixing feature by making various modifications on the available chaotic maps. The researchers have constructed some general frameworks to get new chaotic maps with increased complexity and improved performances in some applications, including mixing two 1D maps (Garasym *et al.* (2016)), weakly or cross-coupling of 1D chaotic maps (Ablay (2016)), parameter switching based combination of multiple chaotic maps (Wang and Liu (2021)), mixing linear-nonlinear coupled map lattices (Zhou *et al.* (2014)), sine transform of chaotic maps (Hua *et al.* (2019a)), polynomial combination of chaotic maps (Asgari-Chenaghlu *et al.* (2019)), beta-function-based chaotification (Zahmoul *et al.* (2017)), modulo transform based chaotification (Hu and Li (2021); Hua *et al.* (2020); Murillo-Escobar *et al.* (2017); Zhou *et al.* (2014)), modulo operator based generalized Newton complex map (Jafari Barani *et al.* (2020)), cosine transform based chaotic maps (Hua *et al.* (2019b); Liu *et al.* (2016); Talhaoui *et al.* (2021)), composition of chaotic maps with many parameters (Parvaz and Zarebnia (2018)), multi-delayed Chebyshev map (Liu *et al.* (2016)), improvement in chaotic maps with a perturbed parameter (Xiang and Liu (2020)), combination of chaotic maps with floor operator (Pak and Huang (2017)), and mixing three maps with composition, addition and modulo operators (Lan *et al.* (2018)). Most of these approaches cannot fit the uniform distribution which is the central feature of the random numbers. However, the modulo operator based approaches are capable of producing outputs in the uniform distribution range. In (Zhou *et al.* (2014)), a 1D chaotic system is proposed by summing two 1D chaotic maps followed by a modulo operator. In (Murillo-Escobar *et al.* (2017)), the modulo operator is applied to logistic map and an enhanced

Manuscript received: 6 February 2022,
Revised: 25 February 2022,
Accepted: 26 February 2022.

[1] gunyaz.ablay@agu.edu.tr (**Corresponding Author**)

pseudo-random number generator algorithm is obtained. In (Hua *et al.* (2020)), the modulo N operator is applied to the 2D chaotic maps for getting a bounded transformation and improvement in chaos complexity. In (Jafari Barani *et al.* (2020)), the modulo operator and complex folding functions are utilized to get a generalized Newton complex map. In (Hu and Li (2021)), two 1D chaotic maps are coupled by their control parameters for mixing the chaotic behaviors of the seed maps, and then the modulo operator is applied to get an outcome in the range of standard uniform distribution. In general, these chaotic frameworks as random number sources have varying features affecting the throughput efficiency and complexity of the post-processing steps. Most of these chaotic frameworks use several parameters or functions that are not easy to adjust. Some of these chaotic frameworks are completely dependent on the seed chaotic map, and may not produce high quality outputs for other maps.

In this work, a chaotic framework based on a nonlinear transformation via a gain plus modulo-1 operator is proposed to obtain highly complex chaotic behaviors with Lyapunov exponent enhancements and to satisfy the standard uniform distribution $U(0,1)$. The Lyapunov exponent of the chaotic maps and complexity of modulo operator based methods are significantly improved with a gain parameter in this work. The proposed method uses one- or higher-dimensional chaotic maps as seeds and produces completely new chaotic sequences. The method eliminates the time-consuming post-processing steps in chaos-based random number generators. The produced novel chaotic systems significantly broaden the chaotic range of the seed discrete chaotic systems. In addition, the approach removes the periodic windows of existing chaotic systems, and produces robust chaos for practical applications. The uniformity and independence of the chaotic sequences are assured with statistical analyses. The efficiency and feasibility of the proposed approach are illustrated with the random bit generations and image encryption applications.

A GAIN PLUS UNIFORM DISTRIBUTION MODULO ONE TRANSFORMATION IN CHAOTIC MAPS

There is a sea of chaotic maps available for statistical studies, modeling, simulations, cryptography and some other technological applications. These chaotic maps or in general discrete-time chaotic systems can be utilized to generate shaped chaotic algorithms with nonlinear transformations for direct usage in applications including information technologies. Therefore, two main goals of this work are Lyapunov exponent enhancement and achievement of standard uniform distribution in chaotic maps. Consider a discrete-time chaotic map described by

$$x_{k+1} = f(\sigma, x_k) \tag{1}$$

where $f(\cdot)$ represents a real function, $f : R \to R$, and σ is a real-valued parameter. The existence of chaos in any system is usually shown with positive Lyapunov exponent (LE) calculations (Vallejo and Sanjuán (2019)). LEs are computed to characterize the rate of separation of infinitesimally close trajectories, and a positive LE is a requirement for existence of chaos. The positive LE calculation methods start with exponential divergence of nearby trajectories when the trajectory is on the attractor (Awrejcewicz *et al.* (2018)). An exponential separation of nearby phase-space trajectories is given by

$$d_k \approx d_0 e^{\lambda_s k} \tag{2}$$

where λ_s is the LE, d_k is the trajectory separation after k iterates, and d_0 is the initial trajectory separation. By taking the logarithm of both sides and using the property $d_k = f^k(x_0 + d_0) - f^k(x_0)$ for an initial condition x_0, the LE for chaotic map (1) can be given by

$$\lambda_s = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \log |f'(x_k)| \tag{3}$$

where $f' = df/dx$ and it defines the variational (linearized) map as

$$u_{k+1} = f'(x_k) u_k \tag{4}$$

where $u_0 \neq 0$. A positive λ_s indicates the presence of chaos in general. The positive LE is also used to measure unpredictability of the chaotic dynamics in Kolmogorov-Sinai entropy (KSE) calculations.

Definition 1 (Pesin's theorem) (Dorfman (1999)): For an ergodic map, the KSE is equal to the sum of the positive LEs and given by

$$h_{KSE} = \sum_n \lambda_s^+ \tag{5}$$

Similarly, the Ruelle's inequality (Ruelle (1997)) states that the KSE is always less than or equal to the sum of the positive LEs, that is $h_{KSE} \leq \sum_n \lambda_s^+$. This definition indicates that for chaotic maps, the greater LE means the greater KSE and the higher randomness. This gives an idea that if we can increase the values of positive LEs, then more complex chaotic information can be obtained. It is possible to enhance the value of positive LE by nonlinear transformation of the chaotic map (1).

An LE-enhanced uniform distribution modulo one transformation of (1) with a gain α and $\mod 1$ operator is proposed as

$$x_{k+1} = \alpha f(\sigma, x_k) \mod 1 \tag{6}$$

where α is a real-valued gain defined as $\alpha > 1$, $\mod 1$ denotes keeping of the fractional part, $f(\cdot)$ represents the seed chaotic map (1), and the new LE-enhanced chaotic map holds $[0,1] \to [0,1]$. The first goal is the LE enhancement, which can be shown with LE calculations.

Theorem 1: Let the LEs of seed map (1) and transformed map (6) be λ_s and λ, respectively. Then, these LEs are related with $\lambda > \lambda_s$ for $\alpha > 1$.

Proof: For the proposed chaotic map (6), since the linearization slope is $\alpha f'(x_k)$, the LE is given by

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \log |\alpha f'(x_k)| \tag{7}$$

The equation (7) can be expanded as

$$\begin{aligned} \lambda &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \log |f'(x_k)| + \frac{1}{N} \sum_{k=0}^{N-1} \log \alpha \\ &= \lim_{N\to\infty} \frac{1}{N} \log |u_N| + \frac{1}{N} \log \alpha^N \\ &= \lambda_s + \log \alpha \end{aligned} \tag{8}$$

where u_N is computed from the variational map (4) and we have $\lambda > \lambda_s$ since $\alpha > 1$.

This means that the Lyapunov exponent of (6) takes higher values than the seed chaotic map (1) so that a more complex chaotic behavior can be obtained. High-dimensional maps can be obtained by weakly-coupling or cross-coupling of the one-dimensional (1D) chaotic maps (Ablay (2016)). For example, the same or different 1D chaotic maps can be used to create the weakly-coupled (WC) maps as given below

$$\begin{aligned} x_{k+1} &= f_1(\sigma, x_k) + p y_k \\ y_{k+1} &= f_2(\sigma, y_k) - p x_k \end{aligned} \tag{9}$$

where $f_1(\cdot)$ and $f_2(\cdot)$ represent 1D chaotic maps, and p is a small coupling coefficient. The maximal one-dimensional LE of this map is given by (Pikovsky and Politi (2016))

$$\lambda_c = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \log \|F'(x_k, y_k)\| \tag{10}$$

and F' denotes the Jacobian matrix and it defines the variational (linearized) map as

$$\begin{bmatrix} u_{k+1} \\ v_{k+1} \end{bmatrix} = F'(x_k, y_k) \begin{bmatrix} u_k \\ v_k \end{bmatrix} \tag{11}$$

where $u_0, v_0 \neq 0$. An LE-enhanced uniform distribution modulo one transformation of coupled-chaotic map (9) is proposed as

$$\begin{aligned} x_{k+1} &= \alpha(f_1(\sigma, x_k) + p y_k) \mod 1 \\ y_{k+1} &= \alpha(f_2(\sigma, y_k) - p x_k) \mod 1 \end{aligned} \tag{12}$$

where $\alpha > 1$ is a real-valued gain, mod1 denotes keeping of the fractional part, and the new chaotic map holds $[0,1] \to [0,1]$. It can be shown with LE calculations that the maximum LE of (12) is larger than the seed map (9).

Theorem 2: Let the maximum LEs of seed map (9) and transformed map (12) be λ_c and λ, respectively. Then, these maximum LEs are related with $\lambda > \lambda_c$ for $\alpha > 1$.

Proof: For the proposed chaotic map (12), since the Jacobian matrix of the map is $\alpha F'(x_k, y_k)$, the maximum LE is given by

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \log \|\alpha F'(x_k, y_k)\| \tag{13}$$

By using the entry-wise matrix norm, the maximal one-dimensional LE can be written as

$$\begin{aligned} \lambda &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \log \|F'(x_k, y_k)\| + \frac{1}{N} \sum_{k=0}^{N-1} \log \alpha \\ &= \lim_{N\to\infty} \frac{1}{N} \log\left(|u_N| + |v_N|\right) + \frac{1}{N} \log \alpha^N \\ &= \lambda_c + \log \alpha \end{aligned} \tag{14}$$

where u_N and v_N are computed from the variational map (11) and it is obvious that $\lambda > \lambda_c$ since $\alpha > 1$.

Theorem 2 can be applied to any high-dimensional chaotic maps in order to increase the complexity of chaotic systems.

The second main goal is to ensure that the probability density function of the generated random numbers fits the standard uniform distribution $U(0,1)$, because the $U(0,1)$ is at the center of random variable generation. The applications of this distribution include hypothesis testing, random sampling, finance, etc. However, it is important to note that in any application, there is the unchanging assumption that the probability of falling in an interval of fixed length is constant (Dekking *et al.* (2005)). The proposed LE-enhanced chaotic maps have the features of standard uniform distribution, and this will be demonstrated with histograms, statistical property calculations, entropy and correlation evaluations.

Seed chaotic map examples

Practically all chaotic maps can be considered as a seed map. Three different chaotic maps, cubic, signum and sinh maps (Ablay (2016)), are considered in this work. The cubic map is given by

$$x_{k+1} = \sigma x_k - x_k^3 \tag{15}$$

There are three fixed points, $x_e = (0, \pm\sqrt{\sigma - 1})$ for $\sigma > 1$, and the origin is unstable. A chaotic behavior exists for $2.25 < \sigma < 3$ as seen in Fig. 1a. The signum map is defined by

$$x_{k+1} = -\sigma x_k + sign(x_k) \tag{16}$$

where the $sign(\cdot)$ is defined as $sign(x) = x/|x|$ if $x \neq 0$ and $sign(x) = 0$ if $x = 0$. There are three fixed points with unstable origin, $x_e = (0, \pm 1/(\sigma + 1))$ for $\sigma > 0$. The map is chaotic for $1 < \sigma < 2$ as seen in Fig. 2a. The hyperbolic-sine (sinh) map is defined by

$$x_{k+1} = \sigma x_k - \sinh(x_k) \tag{17}$$

The map has three fixed points at $x_e = (0, \pm\gamma)$ for $\sigma > 1$, where $(\sigma - 1)\gamma - \sinh\gamma = 0$. Again the origin is unstable and a symmetric chaotic behavior is available for $3.1 < \sigma < 3.5$ as illustrated in Fig. 4a. In the following sections, the given 1D chaotic maps (15), (16) and (17) will serve as seed maps for developing LE-enhanced chaotic maps.

Performance analysis of LE-enhanced chaotic maps

Many 1D and coupled chaotic maps are able to produce complex chaotic outputs, but not able to generate uniformly distributed random numbers. The LE-enhanced chaotic maps (6) can solve this problem by increasing the complexity and by producing uniformly distributed numbers. In this section, the performances of the LE-enhanced chaotic maps will be analyzed in terms of the Lyapunov exponents, bifurcation diagrams, histograms, entropies and correlation coefficients.

Lyapunov exponents: LEs of the seed and LE-enhanced chaotic maps are shown in Fig. 1. The seed chaotic maps consist of 1D seed maps (1), i.e., cubic map (15), signum map (16), sinh map (17), and weakly coupled (WC) maps (9). LE-cubic, LE-signum and LE-sinh denote the LE-enhanced maps (6); LEWC-cubic, LEWC-signum and LEWC-sinh maps denote LE-enhanced weakly coupled (LEWC) maps (12). The numerical results are obtained for initial values $x_0 = 0.1234$, $y_0 = 0.1234$ and $p = 0.01$ for the 1D and WC chaotic maps. The gain parameter is taken as $\alpha = 1 \times 10^5$ for LE-cubic and LEWC-cubic maps and $\alpha = 1 \times 10^2$ for LE-signum, LE-sinh, LEWC-signum and LEWC-sinh maps. The LEs of enhanced chaotic maps (blue), compared with the LEs of seed chaotic maps (red), have a broad range of positive LE values. As explained and proved above, the LE enhanced chaotic maps have larger positive LE values than the seed maps, and thus they can exhibit much more complex chaotic behavior. The LE spectrum results given in Fig. 1 are compatible with the bifurcation diagrams (see Fig. 4).

For comparison purposes, the LEs of various models are provided in Fig. 2. The proposed LE-enhanced approach is compared with the unit transform based models given in Refs. (Hu and Li (2021); Zhou *et al.* (2014)), the sine transform based model given in Ref. (Hua *et al.* (2019a)) and the cosine transform based model given in Ref. (Hua *et al.* (2019b)). In the LE computations, summation of two different seed chaotic map functions, $f_1(\sigma_1, x_k) + f_2(\sigma_2, x_k)$ (i.e., cubic + signum, cubic + sinh, and signum + sinh map functions), are utilized to obtain seed chaotic maps, because the given reference studies use this form. Namely,

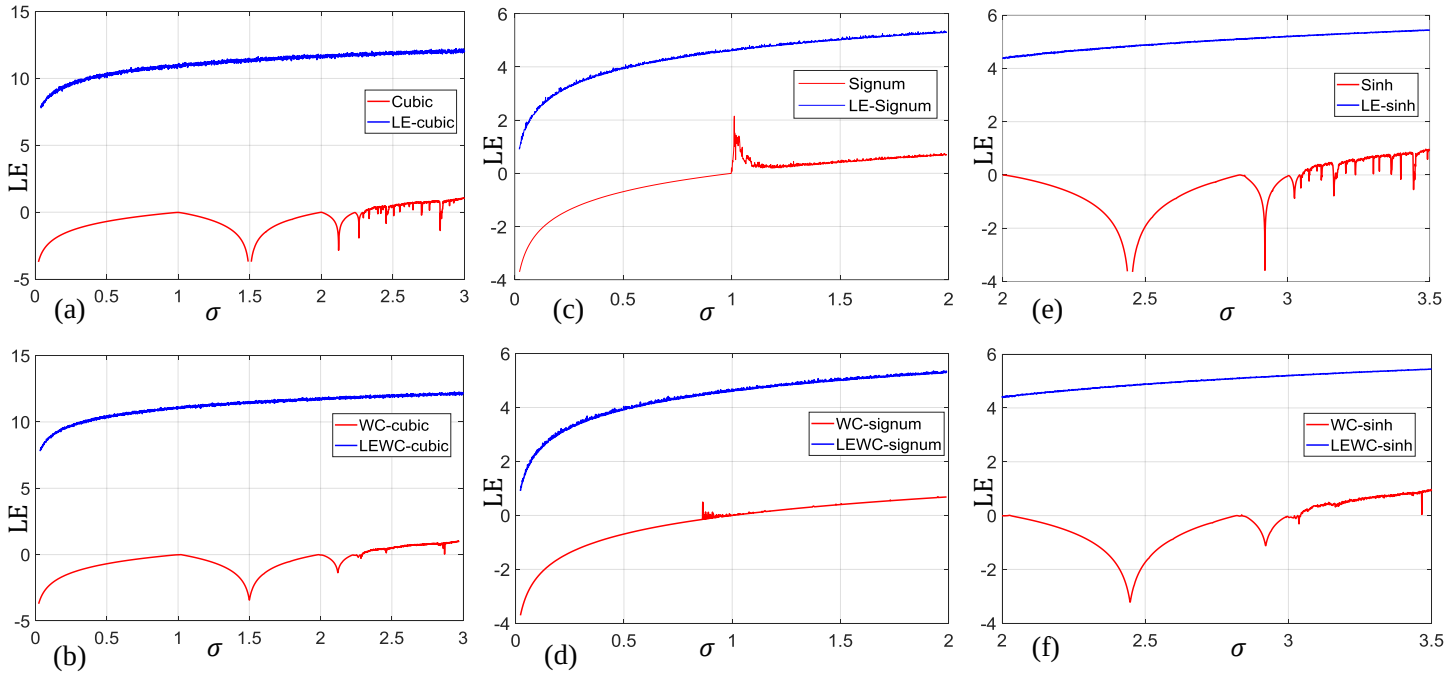

Figure 1 Lyapunov exponents (λ vs σ); (a) cubic maps, (b) weakly-coupled cubic maps; (c) signum maps, (d) weakly-coupled signum maps; (e) sinh maps, (f) weakly-coupled sinh maps.

by considering the LE-enhanced map (6) two different map functions are integrated with the addition operator as

$$x_{k+1} = \alpha(f_1(\sigma_1, x_k) + f_2(\sigma_2, x_k)) \mod 1 \tag{18}$$

where the functions f_1 and f_2 represent different seed chaotic map functions defined in right hand-sides of (15), (16) and (17). It is seen from Fig. 2 that the proposed LE-enhanced chaotification approach provides positive LE values in all parameter ranges of the seed maps. On the other hand, the models provided in Refs. (Hu and Li (2021); Hua *et al.* (2019b,a); Zhou *et al.* (2014)) have seed map dependent efficiency such that Fig. 2c shows that these methods are not valid when the signum + sinh map is the seed map. The efficiency of unit transform (modulo operator) based method is significantly improved with a gain operator in this work, and it is obvious that the proposed method has the best performance among the given methods.

The effect of gain operator α can be illustrated on the cubic map. Figure 3 shows the LEs and bifurcation diagrams of the cubic map (15), LE-enhanced cubic map (6) for $\alpha = 1$ and LE-enhanced cubic map (6) for $\alpha = 1 \times 10^5$. When the gain is $\alpha = 1$, then only mod 1 operator is implemented, and compared with Fig. 3a, it is clear from Fig. 3b that the modulo operator transforms the data to $x \in [0, 1]$, but slightly improves the chaotic features or randomness of data. On the other hand, when the gain is $\alpha = 1 \times 10^5$, then the gain plus mod 1 operator is implemented, and the chaotic and randomness features of the map are significantly improved because LE is always positive and there are no periodic windows in the bifurcation diagram as seen in Fig. 3c.

Bifurcation diagrams: Bifurcation diagrams of the seed maps (1) and (9) and LE-enhanced chaotic maps (6) and (12) are illustrated in Fig. 4. For $\sigma \in [1.5, 3]$, the cubic (15) and WC-cubic (12) maps exhibit a period-doubling route to chaos (Figs. 4a and 4c), but the LE-cubic (6) and LEWC-cubic (12) maps exhibit chaotic behavior within the whole parameter ranges (Figs. 4b and 4d). Besides, the outputs of LE-enhanced chaotic maps fit the range of standard uniform distribution (i.e., $x_k \in [0, 1]$). The signum map for $\sigma \in [0.5, 2]$ and hyperbolic-sine map for $\sigma \in [2.5, 3.5]$ also exhibit similar behaviors as seen in Figs. 4e-4l. It is seen that the WC-chaotic maps increase complexity of the maps, but still we can observe non-uniform distributions and periodic windows. However, the LE-enhanced chaotic maps (6) and (12) provide excellent chaotic features compared with the seed chaotic maps (1) and (9). Note that, the LEWC-chaotic maps (12) provide more complex chaos compared with the 1D LE-chaotic maps (6). For example, the LE-signum map (Fig. 4f) encounters collapse (trajectory approaches to fixed point in long-term run) at $\sigma = 1$, but the LEWC-signum map (Fig. 4h) has no collapse.

Phase diagrams: Phase diagrams of the seed and LE enhanced chaotic maps are illustrated in Fig. 5. The 1D chaotic maps have the data points that are spread evenly across the symmetric lines. The weakly-coupled (WC) chaotic maps increase complexity (randomness) of the chaotic data, but have non-uniform distributions (Figs. 5b,f,j). On the other hand, the phase diagrams of LE-enhanced chaotic maps have completely random data distribution and have quite complex and uniformly distributed chaotic properties.

Entropy and correlation coefficients: The splitting of the outcome space converts the chaotic map into an ergodic information source. Therefore, it is quite convenient to utilize the information theory for analyzing this source. The average level of randomness in the outcome of a variable is determined by the entropy in information theory.

Definition 2 (Shannon entropy) (Karmeshu and Pal (2003)): Entropy H_m of the ensemble $(X_1, p_1), \ldots, (X_m, p_m)$ is given by the expression

$$H_m(p) = -\sum_{i=1}^{m} p_i \log(p_i) \tag{19}$$

where p_i denotes the probability mass associated with the variable

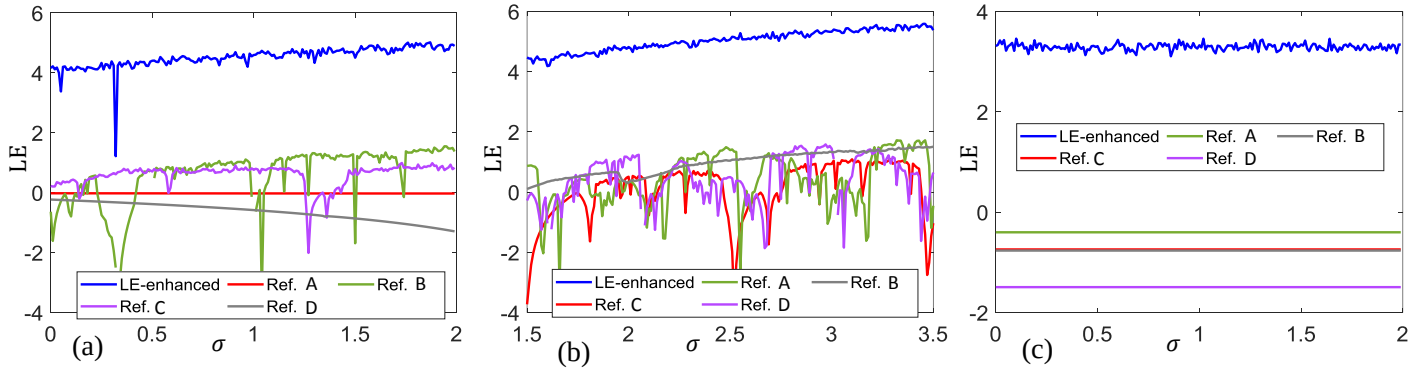

Figure 2 Comparison of Lyapunov exponents (λ vs σ) of different models; (a) cubic+signum, (b) cubic+sinh, and (c) signum+sinh map functions. (Ref.A: Hua *et al.* (2019b), Ref.B: Hu and Li (2021), Ref.C: Zhou *et al.* (2014), Ref.D: Hua *et al.* (2019a))

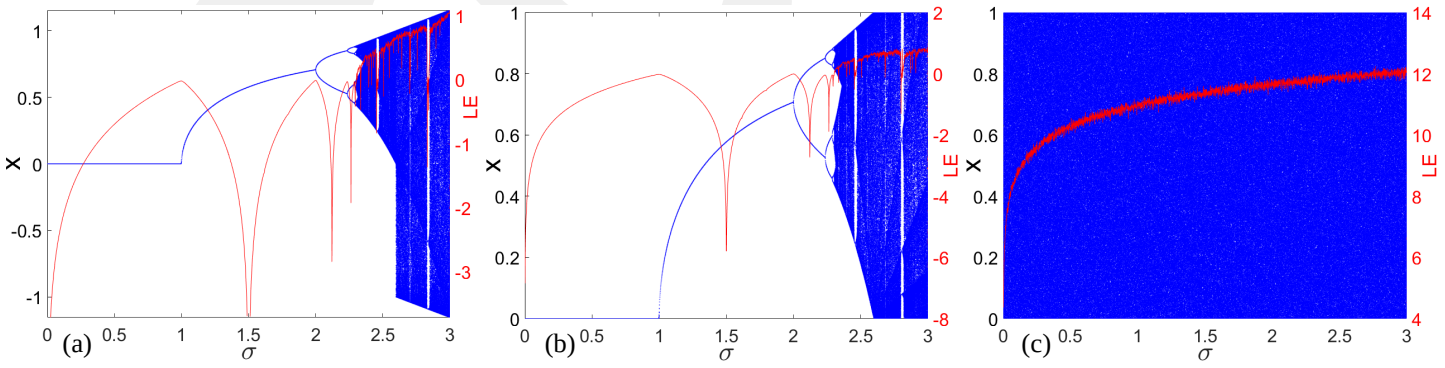

Figure 3 Lyapunov exponents (red) and bifurcation diagrams (blue); (a) cubic seed map, (b) LE-enhanced cubic map with $\alpha = 1$ and (c) LE-enhanced cubic map with $\alpha = 1 \times 10^5$.

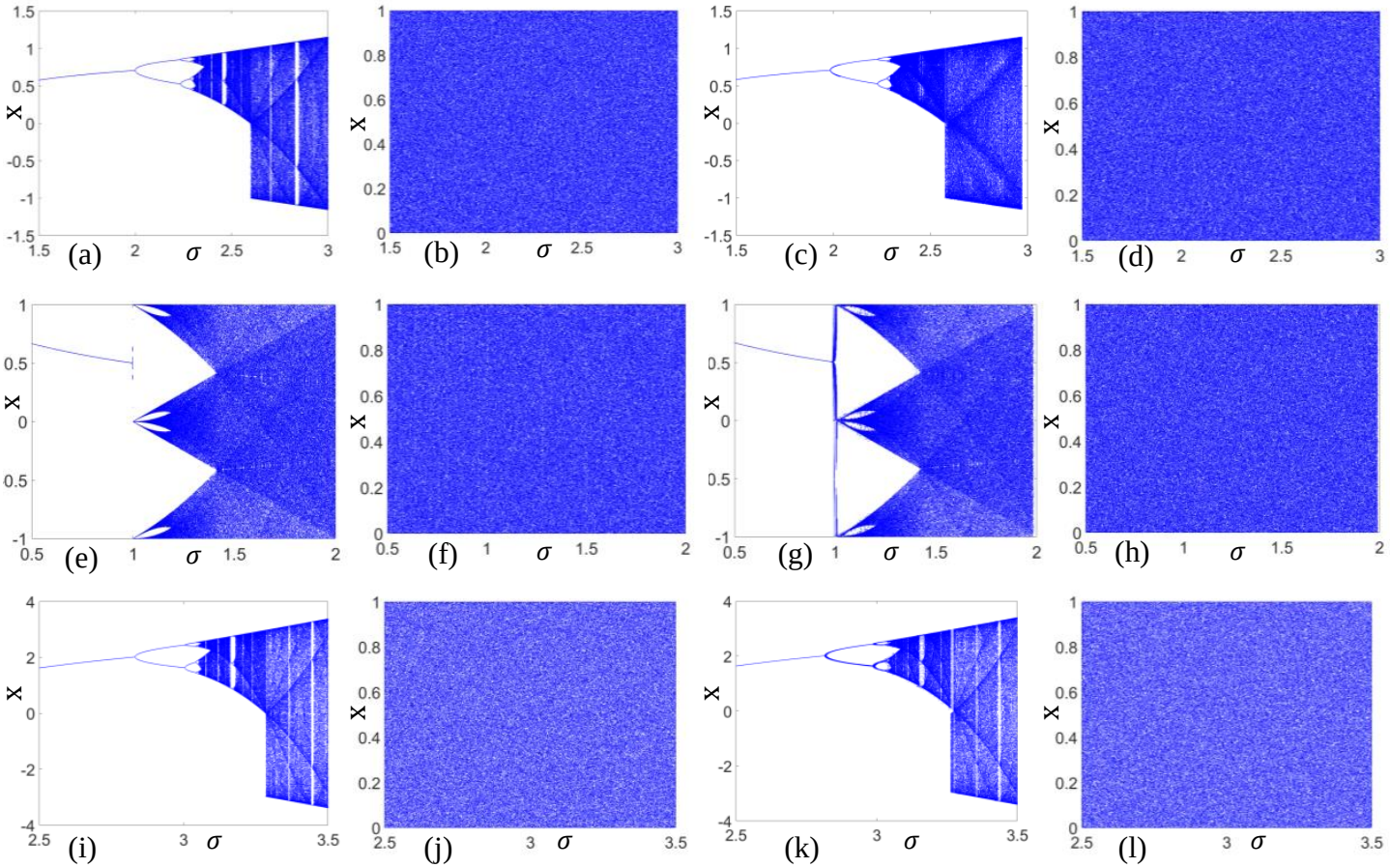

Figure 4 Bifurcation diagrams (x_k vs σ); (a) cubic seed map, (b) LE enhanced cubic map, (c) weakly-coupled cubic map, (d) LE enhanced weakly-coupled cubic map; (e) signum seed map, (f) LE enhanced signum map, (g) weakly-coupled signum map, (h) LE enhanced weakly-coupled signum map; (i) sinh seed map, (j) LE enhanced sinh map, (k) weakly-coupled sinh map, and (l) LE enhanced weakly-coupled sinh map.

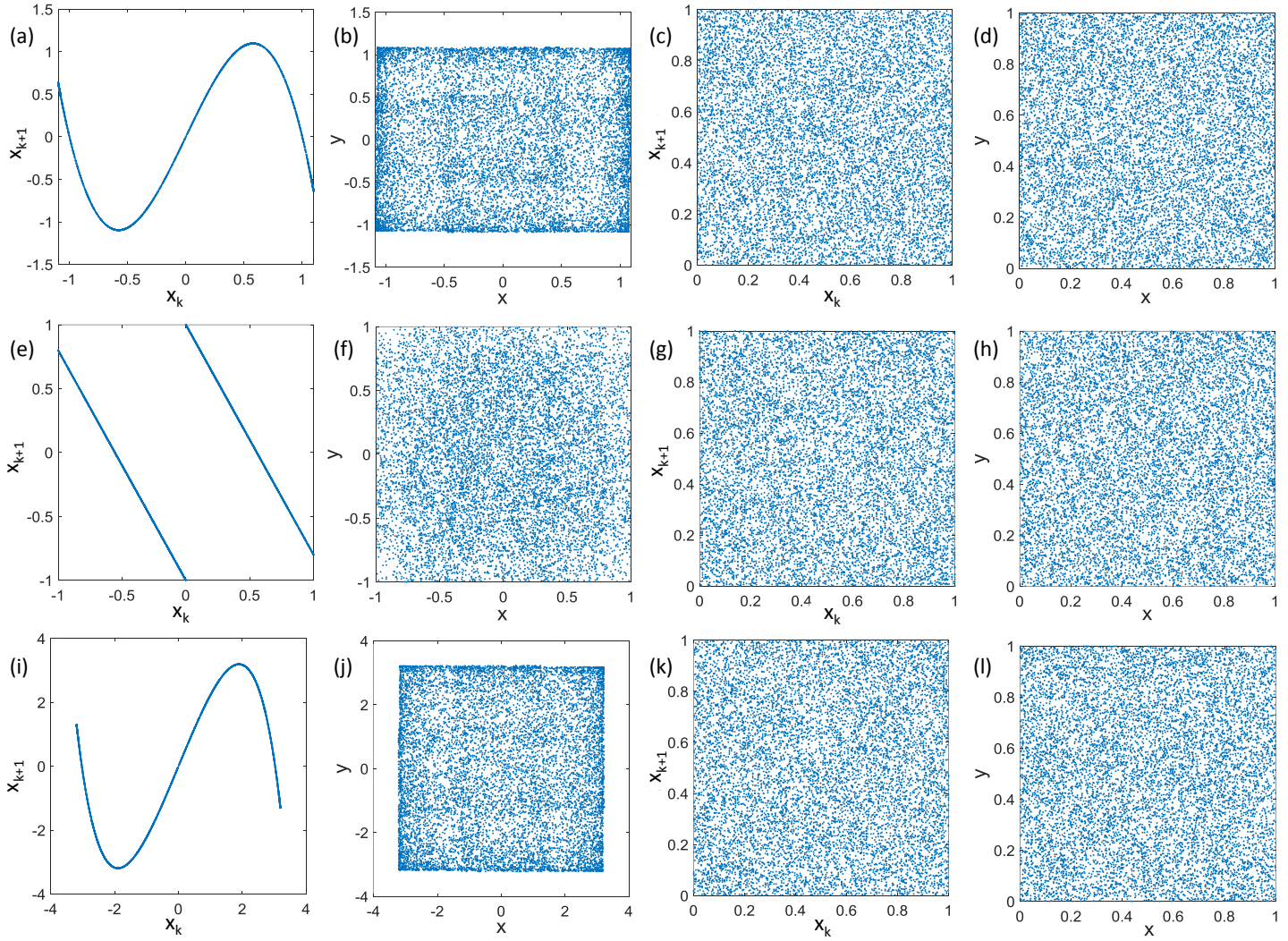

Figure 5 Phase diagrams; (a) cubic map, (b) weakly-coupled cubic map; (c) LE enhanced cubic map, (d) LE enhanced weakly-coupled cubic map, (e) signum map, (f) weakly-coupled sign map; (g) LE enhanced signum map, (h) LE enhanced weakly-coupled signum map, (i) sinh map, (j) weakly-coupled sinh map; (k) LE enhanced sinh map, (l) LE enhanced weakly-coupled sinh map.

X_i such that $\sum p_i = 1$, and the maximum entropy value is given by $H_{max} = \log_2 m$. This definition of the Shannon entropy has a relation with KSE in terms of its supremum as (Falniowski (2014))

$$h_{KSE} = \sup_X \lim_{m\to\infty} \frac{1}{m} H_m(p) \tag{20}$$

The KSE can be interpreted as a generalization of Shannon entropy. Both entropies measure the unpredictability of a deterministic system, and the higher the entropy means the higher the unpredictability. Deciding if generated chaotic sequences are statistically independent can be tested with many statistical test methods. The correlation coefficient is one of these methods that must be satisfied by the chaotic random number generators.

Definition 3 (Correlation coefficient) (James (2006)): For two random variables (x, y) with n observations, the correlation coefficient is defined as

$$R(x,y) = \frac{1}{n-1}\sum_{i=1}^{n}\left(\frac{x_i-\mu_x}{\sigma_x}\right)\left(\frac{y_i-\mu_y}{\sigma_y}\right) \tag{21}$$

where μ_x and μ_y are the means, and σ_x and σ_y are the standard deviations of x and y. The correlation coefficient of two random variables is a measure of their linear independence, and it can be positive, negative or zero. The maximum value of correlation coefficient is $|R| = 1$. Hence, the absolute value of correlation coefficient should be around zero for high random outcomes.

Table 1 shows the calculated entropy and correlation coefficient values. In the probability mass calculations, 1000 subintervals are taken into account, and thus the maximum entropy value is $H_{max} = 9.9658$. As seen in Table 1, the entropies of all chaotic maps are very high, but the LE-enhanced chaotic maps provide almost the maximimum entropy value. The correlation coefficient is calculated for very small initial value differences. The initial conditions are taken as $x_0 = 0.123400$ and $y_0 = 0.123401$ for all chaotic maps. It is seen from Table 1 that all the chaotic maps have almost no correlation since the correlation coefficient is $|R| \approx 0$ for the selected parameter values.

Histograms: The histogram allows measuring the initial condition insensitivity which is related to the splitting of the output space into a number of subintervals, and analyzing the evolution in these regions. Consider a set of equally distributed m subintervals such that

$$X = X_1, \ldots, X_m,\ X_i \cap X_j = \varnothing,\ \text{for } i \neq j \tag{22}$$

Then the randomness in deterministic chaos can be specified through the probabilities. Histogram describes the distribution of the numerical data in each subinterval. The height of each histogram subinterval (or bin) represents the average frequency density for the interval. If the total number of observations are n, the number of subintervals can be calculated from the square-root choice as $m = \sqrt{n}$. The histograms of the chaotic maps are shown in Fig. 6. The total number of observations for each chaotic map are taken as $n = 1 \times 10^6$, so the number of bins can be calculated from the square-root choice as $m = 1000$. Figure 6 displays the histograms of seed cubic, WC cubic, LE-enhanced cubic and LE-enhanced WC cubic maps. The cubic and WC cubic maps have completely non-uniform distributions (Figs. 6a and 6c), while the WC cubic map has a better distribution than the 1D cubic map. On the other hand, the histograms of LE enhanced 1D and WC cubic maps (Figs. 6b and 6d) have a random pattern without any periodic, upward or downward trends. Existence of some significant outliers is an indication of problems in the random number generators. It is clear that there are no obvious outliers in the histograms of LE-enhanced chaotic maps, i.e., data points are spreaded evenly which is a good indication of uniformity. The histograms verify that the data follows the features of standard uniform distribution such that there is almost the same number of observations in each subinterval. Similarly, the histograms of signum, WC signum, sinh and WC sinh maps have non-uniform distributions (Figs. 6e,g,i,k), but their LE-enhanced counterparts have uniformly distributed histograms (Figs. 6f,h,j,l).

Throughout this paper, the system parameters are chosen as follows: $x_0 = 0.1234$ and $y_0 = 0.1234$ for all maps, $\sigma = 2.82$ for cubic maps, $\sigma = 1.8$ for signum maps, $\sigma = 3.4$ for sinh maps, $\alpha = 1 \times 10^5$ for LE-enhanced cubic maps, $\alpha = 1 \times 10^2$ for LE-enhanced signum and sinh maps, $p = 0.01$ for all weakly-coupled (WC) maps.

In practice, the probability density function (pdf) estimations and histograms are closely related. The distribution of the numerical data in each subinterval of the histogram can directly be used to obtain pdf with normalization. Hence, the histograms provide a visual assessment on the pdf estimations. Besides, the statistical properties of the chaotic maps must match the properties of the related distributions. Since the physical origin based random numbers (e.g., radioactive particle emissions) follow the uniform distribution, the LE-enhanced chaotic map should also follow this distribution. The statistical properties of the standard uniform distribution $U(0,1)$ are given by $mean = 0.5$, $median = 0.5$, $variance = 0.0833$, $skewness = 0$, $kurtosis = 1.8$, $pdf = 1$ and $cdf = x$ for $x \in [0,1]$. The probability of falling in the interval of fixed length $[0,1]$ is constant in the uniform distribution. Table 1 shows the statistical properties of chaotic maps for total number of observations $n = 1 \times 10^6$. It is seen that the LE-enhanced chaotic maps successfully follow the statistical properties of standard uniform distribution $U(0,1)$. Note that the parameters α and σ of LE-enhanced chaotic maps ((6) and (12)) have significant effects on the randomness features of chaotic sequences, so they should be selected suitably in practical applications.

APPLICATIONS

LE-enhanced chaotic maps as random bit generators

Random bit generators are significant for many applications in statistical physics, stochastic modeling, numerical simulations, and cryptography. A random bit generator must provide statistically independent and unbiased bits (namely, fully unpredictable bits). The ranges of sequences produced from most of the chaotic systems do not match the random bit generator requirements, so many authors have proposed chaotic map specific post-processing algorithms (Pulido-Luna *et al.* (2021); Jafari Barani *et al.* (2020); Hamza (2017)). On the other hand, since the proposed LE-enhanced chaotic maps produce uniformly distributed random numbers, a binary converter algorithm can directly be used to generate random bits, such as a comparator is defined by

$$b_k = \begin{cases} 1 & \text{if } x_k \geq 0.5 \\ 0 & \text{otherwise} \end{cases} \tag{23}$$

where b_k represents random bits, $b_k \in \{0,1\}$, and the threshold is selected as the mean value of the LE-enhanced chaotic maps (6). If a chaotic system is not providing uncorrelated and unbiased bits, the de-skewing techniques (Stallings (2006)) (e.g., Von Neumann technique) can be used to remove possible correlations and biases in the binary sequences. However, the proposed LE-enhanced chaotic maps (6) are able to produce high quality random numbers

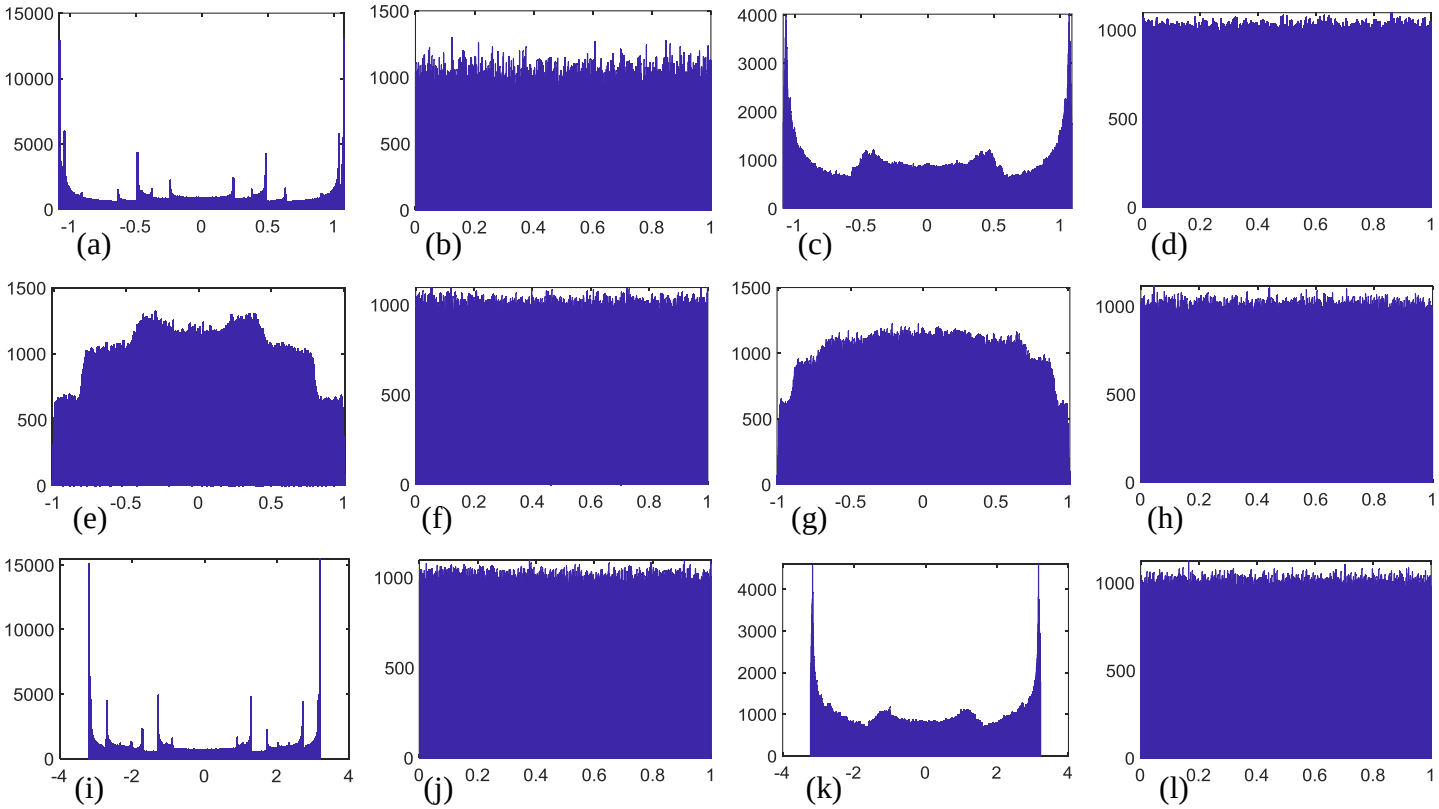

Figure 6 Histograms (counts vs x_k): (a) cubic seed map, (b) LE-enhanced cubic map, (c) weakly-coupled cubic map, (d) LE-enhanced weakly-coupled cubic map; (e) signum seed map, (f) LE-enhanced signum map, (g) weakly-coupled signum map, (h) LE-enhanced weakly-coupled signum map; (i) sinh seed map, (j) LE-enhanced sinh map, (k) weakly-coupled sinh map, and (l) LE-enhanced weakly-coupled sinh map.

Table 1 Randomness test results for the LE-enhanced chaotic maps.

Property	Cubic Map	Sign Map	Sinh Map	WC Cubic Map	WC Sign Map	WC Sinh Map	LE Cubic Map	LE Sign Map	LE Sinh Map	LEWC Cubic Map	LEWC Sign Map	LEWC Sinh Map
Mean	0	0	0.002	0	0	0	0.5	0.5	0.5	0.5	0.5	0.5
Median	0	0	0.005	0	0	0	0.5	0.5	0.5	0.5	0.5	0.5
Variance	0.4784	0.278	4.500	0.4844	0.2771	4.345	0.0837	0.0834	0.0834	0.0834	0.0833	0.0833
Skewness	0.001	0.001	0.002	0.001	0.002	0.001	0.003	0.001	0.003	0.000	0.000	0.001
Kurtosis	1.751	1.947	1.609	1.718	1.948	1.664	1.796	1.799	1.798	1.799	1.799	1.799
Range	(-2,2)	[-1,1]	(-4,3)	(-2,2)	[-1,1]	(-4,4)	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]
Correlation	0.0018	0.0009	0.0013	0.0013	0.0012	0.0003	0.0008	0.0011	0.0008	0.0015	0.0011	0.0005
Entropy	9.7400	9.9334	9.7000	9.8540	9.9363	9.8645	9.9604	9.9650	9.9651	9.9651	9.9651	9.9650

as proved in the previous section, which can eliminate the use of a de-skewing algorithm. This is an important advantage because the post-processing steps are eliminated. This is an advantage in terms of less time consuming and short algorithm developments, for instance, the random bit generation can easily be implemented with in-line codes rather than function calls. More importantly, the usage of a de-skewing technique provides less than 25% efficiency with respect to the random bit throughput, but the proposed LE-enhanced approach has 100% efficiency.

The commonly used statistical testing methods for randomness analysis of binary values are provided in NIST SP 800-22 test suite (Bassham *et al.* (2010)). The output file containing 5120000 random bits are generated to be tested with the NIST statistical test suite. The test results are given in Table 2. The LE-enhanced chaotic maps successfully pass the statistical tests, implying that these maps can be used in cryptosystems. Clearly, the statistical tests may not determine the quality of the produced random bits alone, but some conclusions can be drawn about it. In practice, the quality of applications must be checked with application specific randomness analysis tests. In addition, since chaotic systems have high sensitivity to initial conditions, for the unpredictability of chaotic random bit generators an efficient approach can be connecting the initial condition of chaotic maps with an input device of the application environment, e.g., thermal noise, port value and mouse movement.

LE-enhanced chaotic maps based Image encryption

The proposed chaotic random bit generators are applied to an image encryption scheme in this section. Today, almost all image encryption schemes use different chaotic systems with many different sophisticated encryption algorithms (Khan and Kayhan (2021); Wang and Liu (2021); Talhaoui *et al.* (2021)). Here, for image encryption and decryption, the key bits are generated from the LE-enhanced sinh map, and the symmetric-key encryption method is implemented. The grayscale image of size KL pixels is converted into one-dimensional array of pixels M_i, $i = 1, 2, .., KL$, and then each M_i pixel is represented with 8-bit blocks (i.e., 256 shades per pixel). Hence, the bit length of binary sequence for the given figure is equal to $K \times L \times 8$ bits. The same number of random bits are generated from the LE-enhanced sinh map and represented with 8-bit blocks for using in the pixel-by-pixel encryption scheme. The XORing operator is implemented between the key and image bit sequences for encryption. For decryption of the image, the XORing operator is implemented between the key and decrypted image bit sequences.

Histogram analysis: Histogram of a digital image displays the distribution of grayscale values of all the pixels. For an 8-bit grayscale image there are $2^8 = 256$ different possible intensities, which are visualized by the histograms. Four grayscale images, their encrypted images and corresponding histograms are illustrated in Fig. 7. The histograms of plain-text images are one of the most common cryptosystem attacks (Farajallah *et al.* (2016)), because they exhibit the characteristic properties of the images as seen in Figs. 7b,f,j,n. On the other hand, all the plain-text images become indistinguishable noise-like ciphers after encryption as seen in Figs. 7c,g,k,o. The histograms of four cipher-text images just show indistinguishable and identical properties (see Figs. 7d,h,l,p). All 256 gray levels appear with almost the same probability in encrypted images, and the histograms are not leaking any significant information to the statistical attacks.

The chi-square goodness-of-fit test can be used to determine whether the histogram data sample fits the uniform probability distribution (James (2006)). By taking into account the histogram data, the chi-square test statistic can be calculated as

$$\chi^2 = \sum_{i=1}^{256} (O_i - E_e)^2 / E_e \tag{24}$$

where O_i is the observed counts of gray level i in an image, and $E_e = KL/256$ represents the expected counts for grayscale image of size KL pixels. The test statistic has an approximate chi-square distribution of 256 degrees of freedom, and the hypothesis at the 5% significance level can be accepted if $\chi^2 < \chi^2_{0.05}(256) = 320$, otherwise it can be rejected. The χ^2-test statistics of images shown in Fig. 7 (both plain-text and cipher-text images) are listed in Table 3. It is seen from Table 3 that the statistics of the cipher-text images are small and satisfy the hypothesis, while the plaintext images have much larger values and are not satisfying the hypothesis. This means that the histograms of cipher-text images are approximately uniformly distributed.

Correlation analysis: The correlation between adjacent pixels of an image data is high due to natural image properties. Hence, an image encryption algorithm must eliminate this high correlation and provide an adequate resistance against statistical attacks. To test correlation dimensions of images, 30000 pairs of adjacent pixels from vertical and horizontal directions in plain-text images and cipher-text images are randomly selected, and the corresponding correlation coefficients are calculated using (21) and listed in Table 3. It is seen that the plain-text images have high correlation (around 1) in vertical and horizontal directions. On the other hand, the correlation coefficients of the cipher-text images are approximately zero, indicating that there are almost no correlations between adjacent pixels. That is, the proposed LE-enhanced chaotic maps produce highly random bits.

Mean square error analysis: The difference between original and encrypted image pixels (each pixel has 256 shades of gray) is measured with the mean square error (MSE). The MSE can be defined as

$$MSE = \frac{1}{KL} \sum_{i=1}^{K} \sum_{j=1}^{L} (O_{ij} - E_{ij})^2 \tag{25}$$

where O_{ij} is the original image pixel, E_{ij} is the encrypted image pixel, and K and L represent the pixel size of the original or encrypted image. The MSE result is equal to zero if the images are the same, but it should be as high as possible if the compared images are different. A higher MSE value means the cipher-text image is more immune to attacks. The calculated MSE values for different cipher-text images are tabulated in Table 3. The MSE values are much higher than zero ($MSE \gg 0$), and thus the LE-enhanced chaotic map based encryption provides highly satisfactory results.

Entropy analysis: In the probability mass calculations, 256 subintervals are taken into account, and thus the maximum entropy value is $H_{max} = \log_2 256 = 8$. The formula (19) is used to calculate entropy of cipher-text images. Table 3 shows that the entropy values of the cipher-text images are practically equal to the maximum entropy value (around 8), indicating that the unpredictability level of the cipher-text images is maximum.

Table 2 Randomness (NIST) test results for the LE-enhanced chaotic maps.

Test Name	LE Cubic Map	LE Sign Map	LE Sinh Map	LEWC Cubic Map	LEWC Sign Map	LEWC Sinh Map
Frequency	10/10	10/10	10/10	10/10	10/10	10/10
Block frequency	10/10	10/10	10/10	9/10	10/10	10/10
Cumulative sums Forward	10/10	10/10	8/10	10/10	10/10	9/10
Cumulative sums Reverse	10/10	10/10	9/10	10/10	10/10	10/10
Runs	10/10	9/10	10/10	10/10	10/10	10/10
Longest run	10/10	9/10	10/10	10/10	10/10	10/10
Rank	10/10	10/10	10/10	10/10	9/10	10/10
FFT	10/10	10/10	10/10	10/10	10/10	10/10
Non-overlapping template	10/10	10/10	10/10	10/10	10/10	10/10
Overlapping template	10/10	10/10	10/10	10/10	10/10	10/10
Universal	9/10	9/10	10/10	9/10	10/10	10/10
Approximate entropy	10/10	10/10	9/10	10/10	9/10	10/10
Random excursions	4/4	4/4	2/2	4/4	3/3	5/5
Random excursions variant	4/4	4/4	2/2	4/4	3/3	5/5
Serial	9/10	10/10	10/10	10/10	10/10	10/10
Linear complexity	10/10	10/10	10/10	10/10	10/10	10/10

Table 3 Statistical analysis results of the encrypted images.

Images	Correlation plain-image (vertical)	Correlation cipher-image (vertical)	Correlation plain-image (horizontal)	Correlation cipher-image (horizontal)	χ^2 plain-image	χ^2 cipher-image	MSE	Entropy
coins.png	0.9726	0.0047	0.9676	0.0066	3×10^5	306	21519	7.9969
peppers.png	0.9917	0.0051	0.9860	0.0021	4×10^5	267	21674	7.9990
corn.tif	0.9662	0.0071	0.0514	0.0067	4×10^4	251	21627	7.9986
moon.tif	0.9949	0.0011	0.0282	0.0005	3×10^6	312	21577	7.9988
football.jpg	0.9437	0.0018	0.9347	0.0022	2×10^5	237	21474	7.9979

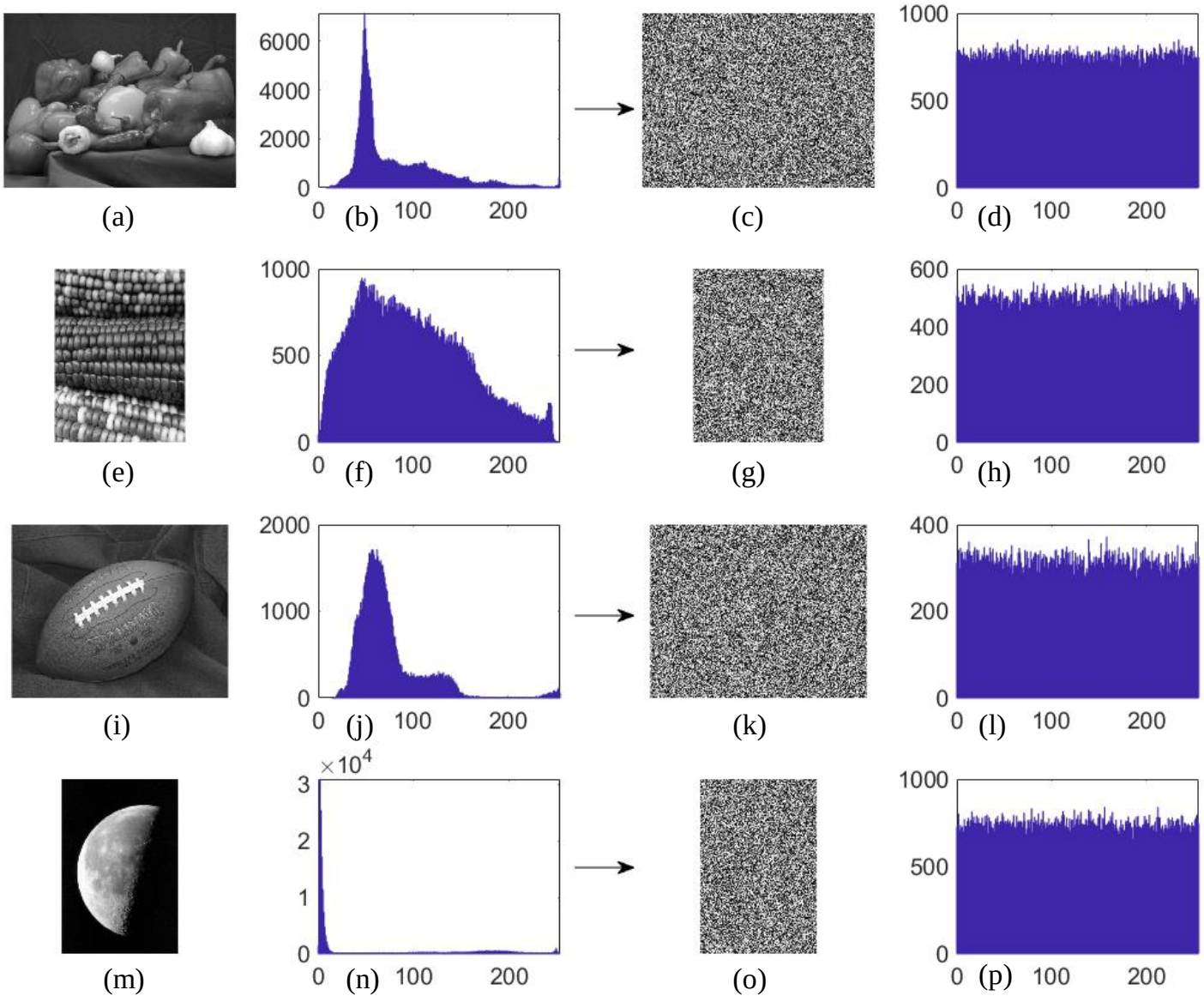

Figure 7 Histogram analysis: (a) peppers; (b) histogram of (a); (c) encrypted peppers; (d) histogram of (c); (e) corn; (f) histogram of (e); (g) encrypted corn (c); (h) histogram of (g); (i) football; (j) histogram of (i); (k) encrypted football; (l) Histogram of (k); (m) moon; (n) histogram of (m); (o) encrypted moon; (p) histogram of (o).

CONCLUSION

The uniformity and statistically independence are two key features that a chaotic random number generator must satisfy for cryptographic and scientific applications. A gain plus modulo-1 operator based chaotic framework is proposed in this work to enhance the Lyapunov exponent of the seed chaotic maps and to assure that the chaotic outcomes follow the standard uniform distribution $U(0,1)$ with highly random chaotic sequences. It is shown that the gain plus modulo-1 operator based approach greatly broadens the chaotic range of seed chaotic maps and generates robust chaos. The proposed approach produces chaotic sequences that are replicable, fast, portable and closely approximate the ideal statistical properties of uniformity and independence. The proposed chaotic framework successfully passes the fundamental statistical and visual tests. The approach can eliminate the use of post-processing approaches (e.g., de-skewing) and provide 100% efficiency with respect to the random bit throughput. The efficiency and feasibility of the approach are verified with an image encryption application. The proposed method has a high potential in science, technology and cryptography applications.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

Availability of data and material

Not applicable.

LITERATURE CITED

Ablay, G., 2016 Chaotic map construction from common nonlinearities and microcontroller implementations. International Journal of Bifurcation and Chaos **26**: 1650121.

Asgari-Chenaghlu, M., M.-A. Balafar, and M.-R. Feizi-Derakhshi, 2019 A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. Signal Processing **157**: 1–13.

Awrejcewicz, J., A. V. Krysko, N. P. Erofeev, V. Dobriyan, M. A. Barulina, *et al.*, 2018 Quantifying Chaos by Various Computational Methods. Part 1: Simple Systems. Entropy **20**: 175.

Banerjee, S., L. Rondoni, and M. Mitra, editors, 2012 *Applications of Chaos and Nonlinear Dynamics in Science and Engineering - Vol. 2*. Springer-Verlag, Berlin Heidelberg.

Bassham, L. E., A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, *et al.*, 2010 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States.

Benamara, O., F. Merazka, and K. Betina, 2016 An improvement of a cryptanalysis algorithm. Information Processing Letters **116**: 192–196.

Dekking, F. M., C. Kraaikamp, H. P. Lopuhaä, and L. E. Meester, 2005 *A Modern Introduction to Probability and Statistics: Understanding Why and How*. Springer-Verlag, London.

Dorfman, J. R., 1999 *An Introduction to Chaos in Nonequilibrium Statistical Mechanics*. Cambridge Lecture Notes in Physics, Cambridge University Press, Cambridge.

El-Hameed, H. A. A., N. Ramadan, W. El-Shafai, A. A. M. Khalaf, H. E. H. Ahmed, *et al.*, 2021 Cancelable biometric security system based on advanced chaotic maps. The Visual Computer .

Falniowski, F., 2014 On the Connections of Generalized Entropies With Shannon and Kolmogorov–Sinai Entropies. Entropy **16**.

Farajallah, M., S. El Assad, and O. Deforges, 2016 Fast and secure chaos-based cryptosystem for images. International Journal of Bifurcation and Chaos **26**: 1650021(1–21).

Garasym, O., I. Taralova, and R. Lozi, 2016 New Nonlinear CPRNG Based on Tent and Logistic Maps. In *Complex Systems and Networks: Dynamics, Controls and Applications*, edited by J. Lü, X. Yu, G. Chen, and W. Yu, Understanding Complex Systems, pp. 131–161, Springer, Berlin, Heidelberg.

Hamza, R., 2017 A novel pseudo random sequence generator for image-cryptographic applications. Journal of Information Security and Applications **35**: 119–127.

Hu, G. and B. Li, 2021 Coupling chaotic system based on unit transform and its applications in image encryption. Signal Processing **178**: 107790.

Hua, Z., Y. Zhang, and Y. Zhou, 2020 Two-Dimensional Modular Chaotification System for Improving Chaos Complexity. IEEE Transactions on Signal Processing **68**: 1937–1949.

Hua, Z., B. Zhou, and Y. Zhou, 2019a Sine Chaotification Model for Enhancing Chaos and Its Hardware Implementation. IEEE Transactions on Industrial Electronics **66**: 1273–1284.

Hua, Z., Y. Zhou, and H. Huang, 2019b Cosine-transform-based chaotic system for image encryption. Information Sciences **480**: 403–419.

Jafari Barani, M., P. Ayubi, M. Yousefi Valandar, and B. Y. Irani, 2020 A new Pseudo random number generator based on generalized Newton complex map with dynamic key. Journal of Information Security and Applications **53**: 102509.

James, F., 2006 *Statistical Methods In Experimental Physics*. World Scientific, Hackensack, NJ, second edition.

Karmeshu and N. R. Pal, 2003 Uncertainty, Entropy and Maximum Entropy Principle — An Overview. In *Entropy Measures, Maximum Entropy Principle and Emerging Applications*, edited by Karmeshu, Studies in Fuzziness and Soft Computing, pp. 1–53, Springer, Berlin, Heidelberg.

Khan, J. S. and S. K. Kayhan, 2021 Chaos and compressive sensing based novel image encryption scheme. Journal of Information Security and Applications **58**: 102711.

Lan, R., J. He, S. Wang, T. Gu, and X. Luo, 2018 Integrated chaotic systems for image encryption. Signal Processing **147**: 133–145.

Liu, L., S. Miao, M. Cheng, and X. Gao, 2016 A pseudorandom bit generator based on new multi-delayed Chebyshev map. Information Processing Letters **116**: 674–681.

Luo, Y., S. Zhang, J. Liu, and L. Cao, 2020 Cryptanalysis of a Chaotic Block Cryptographic System Against Template Attacks. International Journal of Bifurcation and Chaos **30**: 2050223.

Murillo-Escobar, M. A., C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, 2017 A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. Nonlinear Dynamics **87**: 407–425.

Pak, C. and L. Huang, 2017 A new color image encryption using combination of the 1D chaotic map. Signal Processing **138**: 129–137.

Parvaz, R. and M. Zarebnia, 2018 A combination chaotic system and application in color image encryption. Optics & Laser Technology **101**: 30–41.

Pikovsky, A. and A. Politi, 2016 *Lyapunov Exponents: A Tool to Explore Complex Dynamics*. Cambridge University Press, Cambridge.

Pulido-Luna, J. R., J. A. López-Rentería, N. R. Cazarez-Castro, and E. Campos, 2021 A two-directional grid multiscroll hidden attractor based on piecewise linear system and its application in pseudo-random bit generator. Integration **81**: 34–42.

Ruelle, D., 1997 Chaos, predictability, and idealization in physics. Complexity **3**: 26–28.

Stallings, W., 2006 *Cryptography and Network Security: Principles and Practice*. Prentice Hall.

Strogatz, S. H., 2015 *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. CRC Press, Boulder, CO, second edition.

Talhaoui, M. Z., X. Wang, and M. A. Midoun, 2021 A new one-dimensional cosine polynomial chaotic map and its use in image encryption. The Visual Computer **37**: 541–551.

Vallejo, J. C. and M. A. F. Sanjuán, 2019 *Predictability of Chaotic Dynamics : A Finite-time Lyapunov Exponents Approach*. Springer Series in Synergetics, Springer International Publishing, Switzerland, second edition.

Wang, X. and P. Liu, 2021 Image encryption based on roulette cascaded chaotic system and alienated image library. The Visual Computer .

Xiang, H. and L. Liu, 2020 An improved digital logistic map and its application in image encryption. Multimedia Tools and Applications **79**: 30329–30355.

Zahmoul, R., R. Ejbali, and M. Zaied, 2017 Image encryption based on new Beta chaotic maps. Optics and Lasers in Engineering **96**: 39–49.

Zhou, Y., L. Bao, and C. L. P. Chen, 2014 A new 1D chaotic system for image encryption. Signal Processing **97**: 172–182.

How to cite this article: Ablay, G. Lyapunov Exponent Enhancement in Chaotic Maps with Uniform Distribution Modulo One Transformation. Chaos Theory and Applications, 4(1), 45-58, 2022.