Sine Chaotification Model for Enhancing Chaos and Its Hardware Implementation

Zhongyun Hua , *Member, IEEE*, Binghang Zhou, and Yicong Zhou , *Senior Member, IEEE*

Abstract—**When chaotic systems are used in different practical applications, such as nonlinear control and cryptography, their complex chaos dynamics are strongly required. However, many existing chaotic systems have simple complexity, and this brings negative effects to chaos-based applications. To address this issue, this paper introduces a sine chaotification model (SCM) as a general framework to enhance the chaos complexity of existing one-dimensional (1-D) chaotic maps. The SCM uses a sine function as a nonlinear chaotification transform and applies it to the output of a 1-D chaotic map. The resulting enhanced chaotic map of the SCM has better chaos complexity and a much larger chaotic range than the seed map. Theoretical analysis verifies the efficiency of the SCM. To show the performance of the SCM, we apply SCM to three existing chaotic maps and analyze the dynamics properties of the obtained enhanced chaotic maps. Performance evaluations prove that the three enhanced chaotic maps have more complicated dynamics behaviors than their seed chaotic maps. To show the implementation simplicity of the SCM, we implement the three enhanced chaotic maps using the field-programmable gate array. To investigate the SCM in practical application, we design pseudorandom number generators using the enhanced chaotic maps.**

Index Terms—**Chaotic system, chaotification, chaos-based application, cryptography, field-programmable gate array (FPGA) implementation, nonlinear control.**

I. INTRODUCTION

CHAOS theory is a subdiscipline of mathematics and it describes the behaviors of dynamical system that are highly sensitive to initial states [1]. Chaotic behaviors exist in all kinds of natural and man-made scenarios, such as climate, road traffic, and stock marketing [2]–[4]. The dynamical systems owning chaotic behaviors are called chaotic systems. Even though a chaotic system is deterministic, which means that its future behavior is totally determined by its initial state, long-term prediction of its behavior is impossible [5], [6]. Therefore, the chaotic system has many specific properties, such as initial state sensitivity, unpredictability, and topological mixing [7]–[9]. These meaningful properties make chaotic systems widely studied [10]–[12] and have applications in many disciplines, including meteorology, sociology, physics, computer science, engineering, economics, and many others [13], [14]. Following are several examples. As the initial state sensitivity and ergodicity of chaos are similar to the diffusion and confusion properties of cryptography [15], chaotic systems are widely used in designing cryptographic algorithms [16], [17]. When coupling several dissipative chaotic systems, these systems may exhibit synchronization phenomenon and the synchronization of chaos can be used in secure communication [18] and signal detection [19], [20].

Since E. N. Lorenz first built the Lorenz chaotic system to describe the change of weather [21], many chaotic systems have been designed to describe different kinds of chaos phenomena and these chaotic systems can be divided into two categories: discrete-time chaotic system and continuous-time chaotic system. Examples of discrete-time chaotic systems include the logistic map, complex quadratic map, and Hénon map, while examples of continuous-time chaotic systems include the Chua circuit [22], Lü chaotic attractor [23] and memristor-based chaotic oscillating circuits [24], [25]. Except for these well-defined chaotic systems, numerous chaotic models have also been introduced to achieve better chaotic dynamics behaviors [26], [27]. These models can either obtain new dynamical behaviors by perturbing the chaotic signals of existing chaotic maps [28], [29] or generating new chaotic systems [30], [31]. For example, Wang *et al.* proposed a new method of designing high-dimensional digitalized chaotic systems within the finite precision domain in [31]. This method adopts the strategy that uses random sequences to control the chaos generation.

When studying chaos theory and applying chaos theory to different disciplines, researchers found that many existing chaotic systems have performance limitations in different aspects. First, with the fast development of discerning chaos technologies, the behaviors of many existing chaotic systems can be evaluated by identifying the initial states [32], [33] or estimating the chaotic signals [34], [35]. Secondly, chaos degradation will

happen when chaotic behaviors are simulated in the domain of finite precision [36]. Theoretically, a chaotic behavior will never close or repeat in the phase plane. However, as the finite precision domain cannot have infinite states, the close states in the phase plane will appear precision truncation and overlap. This makes the chaotic behaviors degrade to periodic behaviors and thus causes negative effects to chaos-based applications [37]. A chaotic system has better performance to defense the chaos degradation if it has better ergodicity. Besides, many existing chaotic maps have frail chaos. Frail chaos means that the chaotic system exhibits chaotic behaviors only in some isolated parameter regions. Slight perturbation to the parameter will make the parameter fall into the nonchaotic regions, and thus will destroy the chaos [38]. Thus, obtaining robust chaos with better chaos performance can significantly promote the research of chaos theory and the development of chaos-based applications [39].

Recently, several chaotic systems have been developed to generate new chaotic maps [40]–[42]. These systems usually generate new chaotic maps by applying nonlinear transforms to existing chaotic maps, which are called seed maps. For example, a parameter-control chaotic system was developed in [40]. It can produce new one-dimensional (1-D) chaotic maps using the outputs of a 1-D chaotic map to change the parameter(s) of another 1-D chaotic map. However, these developed chaotic systems have some limitations. First, these systems should use two or more existing chaotic maps as seed maps. Secondly, the nonlinear transforms of these systems are usually too complex. Moreover, if one of the seed maps has frail chaos performance, the obtained new chaotic maps may not result in good chaos performance.

To enhance the chaos complexity of existing 1-D chaotic maps and obtain robust chaos, this paper proposes a sine chaotification model (SCM). Applying a sine function as a nonlinear chaotification transform to the outputs of a 1-D chaotic map, the SCM not only can enhance the chaos complexity of the original chaotic map in the chaotic range, but also can produce chaos in the nonchaotic range. Different from the developed chaotic systems that have complex nonlinear frameworks and use two or more existing chaotic maps as seed maps, the SCM is a simple but effective framework that is applied to one existing chaotic map. Theoretical and experimental analysis results verify the efficiency and effectiveness of the SCM. The main contributions and novelties of this paper are summarized as follows.

1) We introduce SCM as a universal framework that is able to enhance the chaos complexity of any 1-D chaotic map.
2) The efficiency of the SCM is theoretically analyzed using the concept of Lyapunov exponent (LE).
3) To exhibit the efficiency of the SCM, we apply SCM to three existing 1-D chaotic maps and discuss the chaos dynamics of the obtained enhanced chaotic maps.
4) We experimentally test the chaos performance of these enhanced chaotic maps using the LE, SE, and CD.
5) To demonstrate the simplicity of the SCM in hardware environment, we design and test the circuits of the three enhanced chaotic maps in field-programmable gate array (FPGA) platform.
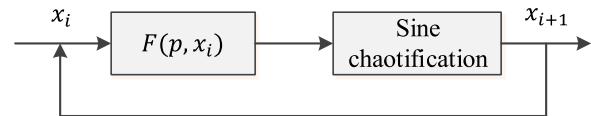

Fig. 1. Structure of the SCM.

6) Pseudorandom number generators (PRNGs) are designed to show the practical application of the SCM.

The remainder of this paper is organized as follows. Section II presents the proposed SCM and analyzes its chaos complexity. Section III applies SCM to three existing chaotic maps, and discusses the chaos dynamics of the three enhanced chaotic maps. Section IV tests the chaos performance of these enhanced chaotic maps. Section V implements the three enhanced chaotic maps using FPGA implementation. Section VI develops PRNGs using the enhanced chaotic maps of the SCM. Section VII concludes this paper.

II. SINE CHAOTIFICATION MODEL

This section introduces the proposed SCM and analyzes its chaos complexity.

A. Concept of SCM

The proposed SCM is designed to enhance the chaos complexity of existing 1-D chaotic maps. Using a sine function as a nonlinear transform and applying it to the outputs of 1-D chaotic maps, SCM can extremely enhance the chaos complexity of these maps. Fig. 1 plots the structure of the SCM. One can see that $F(p, x_i)$ is an existing chaotic map called the seed map, p is a control parameter, and x_i is the input. The output of $F(p, x_i)$ is used as the input of the sine function to enhance complexity, and also used as the input of the seed map for next iteration.

We can use a mathematical equation to present SCM as

$$x_{i+1} = \mathbb{E}(x_i) = \sin(\pi F(p, x_i)) \tag{1}$$

where p is a control parameter.

The sine function has complex nonlinear properties and bounded orbits. It can significantly enhance chaos performance of existing 1-D chaotic maps in a large parameter range. The effectiveness of the sine function in enhancing chaos can be theoretically verified using the principle of LE. Thus, this paper uses the sine function as the chaotification model to enhance chaos. The proposed SCM has the following properties.

1) It is a simple but effective chaotification model that is applied to one existing 1-D chaotic map. Users are flexible to use it to enhance any 1-D chaotic map.
2) The enhanced chaotic maps can overcome the weaknesses of many existing chaotic maps in periodic windows and incomplete attractor distributions.
3) The SCM can enlarge the chaotic ranges of existing 1-D chaotic maps. Most existing 1-D chaotic maps have chaotic behaviors only in a quite small parameter range. However, their enhanced chaotic maps by SCM can own chaotic behaviors in quite large parameter ranges.

These properties will be theoretically analyzed in Section II-B and be experimentally verified in Section IV.

B. Chaos Complexity Analysis

As chaotic behaviors are some observed phenomena, there are no universal standards or mathematical definitions to judge the existence of chaos. The LE [26], [43] is a theoretical description about the existence of chaos and it is one of the most widely used criteria accepted by different researchers. The LE of a difference equation $x_{i+1} = f(x_i)$, denoted as $\lambda_{f(x)}$, is mathematically defined as

$$\lambda_{f(x)} = \lim_{n \to \infty} \left\{ \frac{1}{n} \ln \left| \frac{f^n(x_0 + \epsilon) - f^n(x_0)}{\epsilon} \right| \right\} \quad (2)$$

where ϵ is a very small positive value closing to zero.

Essentially, the LE measures the average divergence of two trajectories starting from two extremely close initial points as the time increases to infinity. When $\lambda_{f(x)} > 0$, trajectories beginning from close initial points exponentially separate in each iteration and will eventually evolve to totally different trajectories. Thus, the dynamical system $f(x)$ can achieve chaotic behavior if $\lambda_{f(x)} > 0$, and larger LE indicates better chaos performance.

Here, we use LE to analyze the chaos complexity of the SCM. Suppose there is a difference equation $x_{i+1} = \hat{\mathbb{S}}(x) = \sin(\pi x_i)$, the SCM defined in (1) can be regarded as a compound function $\hat{\mathbb{S}}(x) \circ F(p, x_i)$. Then, (1) can be rewritten as

$$x_{i+1} = \mathbb{E}(x_i) = \hat{\mathbb{S}}(F(p, x_i)). \quad (3)$$

To calculate LE of the SCM, we suppose x_0 and y_0 are two initial values of (3) and $y_0 = x_0 + \epsilon$, where ϵ is a small positive value. After first iteration, the difference between x_1 and y_1 can be calculated as

$$|x_1 - y_1| = |\mathbb{E}(x_0) - \mathbb{E}(y_0)|$$

$$= \left| \hat{\mathbb{S}}(F(p, x_0)) - \hat{\mathbb{S}}(F(p, y_0)) \right|$$

$$= \left| \frac{\hat{\mathbb{S}}(F(p, x_0)) - \hat{\mathbb{S}}(F(p, y_0))}{F(p, x_0) - F(p, y_0)} \right| \left| \frac{F(p, x_0) - F(p, y_0)}{x_0 - y_0} \right|$$

$$|x_0 - y_0|. \quad (4)$$

Because $y_0 \to x_0$, $F(p, y_0) \to F(p, x_0)$. Then

$$\frac{F(p, x_0) - F(p, y_0)}{x_0 - y_0} \approx \frac{dF}{dx}|_{x_0}$$

$$\frac{\hat{\mathbb{S}}(F(p, x_0)) - \hat{\mathbb{S}}(F(p, y_0))}{F(p, x_0) - F(p, y_0)} \approx \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_0)}.$$

Thus

$$|x_1 - y_1| \approx \left| \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_0)} \right| \left| \frac{dF}{dx}|_{x_0} \right| |x_0 - y_0|.$$

Similarity, after the second iteration, the difference between x_2 and y_2 can be calculated as

$$|x_2 - y_2| = |\mathbb{E}(x_1) - \mathbb{E}(y_1)|$$

$$= \left| \hat{\mathbb{S}}(F(p, x_1)) - \hat{\mathbb{S}}(F(p, y_1)) \right|$$

$$= \left| \frac{\hat{\mathbb{S}}(F(p, x_1)) - \hat{\mathbb{S}}(F(p, y_1))}{F(p, x_1) - F(p, y_1)} \right| \left| \frac{F(p, x_1) - F(p, y_1)}{x_1 - y_1} \right|$$

$$|x_1 - y_1|$$

$$\approx \left| \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_1)} \right| \left| \frac{dF}{dx}|_{x_1} \right| \left| \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_0)} \right| \left| \frac{dF}{dx}|_{x_0} \right| |x_0 - y_0|. \quad (5)$$

After nth ($n \to \infty$) iteration, the difference between x_n and y_n can be calculated as

$$|x_n - y_n| = |\mathbb{E}(x_{n-1}) - \mathbb{E}(y_{n-1})|$$

$$\approx \prod_{i=0}^{n-1} \left| \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_i)} \frac{dF}{dx}|_{x_i} \right| |x_0 - y_0|. \quad (6)$$

Then, the average divergence in the n iterations, denoted as $\Delta_{\mathbb{E}(x)}$, can be calculated as

$$\Delta_{\mathbb{E}(x)} = \left| \frac{x_n - y_n}{x_0 - y_0} \right|^{1/n}$$

$$= \left\{ \prod_{i=0}^{n-1} \left| \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_i)} \frac{dF}{dx}|_{x_i} \right| \right\}^{1/n}. \quad (7)$$

The LE of $\mathbb{E}(x)$, denoted as $\lambda_{\mathbb{E}(x)}$, is defined as the log of the $\Delta_{\mathbb{E}(x)}$, namely

$$\lambda_{\mathbb{E}(x)} = \ln(\Delta_{\mathbb{E}(x)})$$

$$= \ln \left\{ \prod_{i=0}^{n-1} \left| \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_i)} \frac{dF}{dx}|_{x_i} \right| \right\}^{1/n}$$

$$= \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{d\hat{\mathbb{S}}}{dx}|_{F(p, x_i)} \right| + \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{dF}{dx}|_{x_i} \right|. \quad (8)$$

Similarity, the LE of $\hat{\mathbb{S}}(x)$, denoted as $\lambda_{\hat{\mathbb{S}}(x)}$, and the LE of $F(p, x)$, denoted as $\lambda_{F(p,x)}$, can be calculated as

$$\lambda_{\hat{\mathbb{S}}(x)} = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{d\hat{\mathbb{S}}}{dx}|_{x_i} \right|$$

$$\lambda_{F(p,x)} = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{dF}{dx}|_{x_i} \right|. \quad (9)$$

Thus, the LE of $\mathbb{E}(x)$ in (8) is the combination of LEs of $\hat{\mathbb{S}}(x)$ and $F(p, x)$, and

$$\lambda_{\mathbb{E}(x)} = \lambda_{\hat{\mathbb{S}}(x)} + \lambda_{F(p,x)}. \quad (10)$$

From definition of the sine map (see e.g., [40, eq. (1)]), we can know that $\hat{\mathbb{S}}(x)$ is exactly the sine map with control

parameter $\mu = 1$. According to the previous researches (see e.g., [40, Fig. 1(a)]) that when parameter $\mu = 1$, the sine map is chaotic. If a dynamical system is chaotic, it can achieve a positive LE. Thus, $\lambda_{\hat{\mathbb{S}}(x)} > 0$. Then, the chaotic behavior of the SCM can be analyzed as follows.

1) When the seed chaotic map $F(p, x)$ is chaotic, namely $\lambda_{F(p,x)} > 0$, $\lambda_{\mathbb{E}(x)} = \lambda_{\hat{\mathbb{S}}(x)} + \lambda_{F(p,x)} > 0$, and $\lambda_{\mathbb{E}(x)} > \lambda_{F(p,x)}$. In this case, the enhanced chaotic map by SCM has chaotic behavior and can obtain larger LE than its seed map.

2) When $F(p, x)$ doesn't have chaotic behavior and $\lambda_{F(p,x)} > -\lambda_{\hat{\mathbb{S}}(x)}$, $\lambda_{\mathbb{E}(x)} = \lambda_{\hat{\mathbb{S}}(x)} + \lambda_{F(p,x)} > 0$. Then, the enhanced map by SCM can also obtain chaotic behavior.

3) When $F(p, x)$ doesn't have chaotic behavior and $\lambda_{F(p,x)} \leq -\lambda_{\hat{\mathbb{S}}(x)}$, $\lambda_{\mathbb{E}(x)} = \lambda_{\hat{\mathbb{S}}(x)} + \lambda_{F(p,x)} \leq 0$. The enhanced map doesn't have chaotic behavior.

As a result, the enhanced chaotic map by SCM can always obtain larger LE than its seed map. Even the seed chaotic map doesn't have chaotic behavior, the enhanced chaotic map may also have chaotic behavior. This indicates that the proposed SCM can enhance the chaos complexity of existing chaotic maps in the chaotic ranges, and can also produce chaos in the nonchaotic ranges. These properties will be experimentally verified in Section IV-A.

III. EXAMPLES OF ENHANCED CHAOTIC MAPS

To exhibit the effect of the SCM in enhancing the chaos complexity of existing 1-D chaotic maps, as examples, we apply SCM to the logistic map, sine map, and tent map, and analyze the chaos dynamics of the three enhanced chaotic maps.

The logistic map is developed by biologist to calculate the change of population and it is written as

$$x_{i+1} = \mathbb{L}(x_i) = ax_i(1 - x_i) \tag{11}$$

in which the control parameter a is within the range $[0, 4]$.

The sine map is obtained from sine function and its mathematical equation is written as

$$x_{i+1} = \mathbb{S}(x_i) = \mu \sin(\pi x_i) \tag{12}$$

in which the control parameter μ is within the range $[0, 1]$.

The tent map is a polynomial mapping with degree one. It either folds or stretches an input value according to the range of the input value. The representative form of the tent map can be defined as

$$x_{i+1} = \mathbb{T}(x_i) = \begin{cases} rx_i & \text{for } x_i < 0.5 \\ r(1 - x_i) & \text{for } x_i \geq 0.5 \end{cases} \tag{13}$$

in which r is a control parameter and $r \in [0, 2]$.

A. Enhanced Logistic Map

1) Definition: When applying SCM to the logistic map, namely the seed map $F(p, x)$ in (1) is set as the logistic map in (11), we can obtain the enhanced logistic map and it is
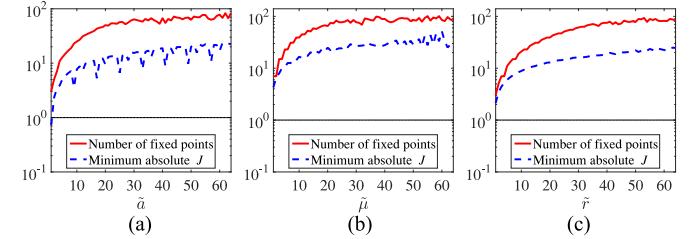

Fig. 2. Number of fixed points with their minimum absolute derivatives. (a) Enhanced logistic map. (b) Enhanced sine map. (c) Enhanced tent map.

defined as

$$x_{i+1} = \mathbb{E}(\mathbb{L}(x_i)) = \sin(\pi \tilde{a} x_i(1 - x_i)) \tag{14}$$

in which $\tilde{a}$ is a control parameter and $\tilde{a} \in (0, +\infty)$.

2) Fixed Point and Stability: A fixed point of a function is one element in the domain of the function which can map to itself by the function. For example, q is a fixed point of the function $f(x)$ only when $f(f(\cdots f(q) \cdots)) = f^n(q) = q$. For a discrete-time chaotic system $x_{i+1} = F(x_i)$, its fixed points are the solutions of the equation $x_i = F(x_i)$. Thus, all the fixed points $\hat{x}$ of the enhanced logistic map can be calculated out using the following equation:

$$\hat{x} = \sin(\pi \tilde{a} \hat{x}(1 - \hat{x})). \tag{15}$$

It is obvious that $\hat{x} = 0$ is a fixed point of the enhanced logistic map in the whole parameter settings. A dynamical system's fixed point can display the stable or unstable state. The stability of a fixed point can be reflected by the gradient of the system at that point. If the corresponding gradient is within the interval $[-1, 1]$, the fixed point shows stable state. Otherwise, it displays unstable state. The gradient of a system's point can be obtained using the corresponding derivative. The derivative of the enhanced logistic map is calculated by

$$J = \frac{dx_{i+1}}{dx_i}$$
$$= \cos(\pi \tilde{a} x_i(1 - x_i))\pi \tilde{a}(1 - 2x_i). \tag{16}$$

Table I lists all the fixed points and their corresponding derivatives of the enhanced logistic map when its parameter $\tilde{a} \in \{1, 2\}$. When $\tilde{a} = 1$, the enhanced logistic map has a fixed point whose derivative is in the range $[-1, 1]$, which indicates that the system is stable. When $\tilde{a} = 2$, all the derivatives of the fixed points are without the interval $[-1, 1]$, which means that the system is unstable. When its parameter $\tilde{a}$ increases, the enhanced logistic map has more fixed points. Fig. 2(a) shows the number of fixed points and their minimum absolute derivatives of the enhanced logistic map when its parameter $\tilde{a} \in [1, 64]$.

When $\tilde{a} \geq 2$, all the minimum absolute derivatives are bigger than one. This indicates that all these fixed points of the enhanced logistic map are unstable. When all the fixed points of a dynamical system are unstable, the system is chaotic.

The bifurcation diagram plots the visited or asymptotically approached values of a chaotic system. Fig. 3(a) displays the bifurcation diagram of the enhanced logistic map when

TABLE I
FIXED POINTS AND THEIR ASSOCIATED DERIVATIVES OF THE ENHANCED LOGISTIC, ENHANCED SINE, AND ENHANCED TENT MAPS

	Fixed points	Associated derivatives
Parameter $\tilde{a}$	Enhanced Logistic map	
1	$\hat{x}_1 = -0.5346$, $\hat{x}_2 = 0.00$, $\hat{x}_3 = 0.6531$	$J(\hat{x}_1) = -5.4930$, $J(\hat{x}_2) = 3.1416$, $J(\hat{x}_3) = -0.7284$
2	$\hat{x}_1 = -0.7690$, $\hat{x}_2 = -0.6690$, $\hat{x}_3 = -0.3341$ $\hat{x}_4 = 0.00$, $\hat{x}_5 = 0.8141$	$J(\hat{x}_1) = -10.1927$, $J(\hat{x}_2) = 10.9234$, $J(\hat{x}_3) = -9.8780$ $J(\hat{x}_4) = 6.2832$, $J(\hat{x}_5) = -2.2931$
⋮	⋮	⋮
Parameter $\tilde{\mu}$	Enhanced Sine map	
1	$\hat{x}_1 = -0.8878$, $\hat{x}_2 = -0.7365$, $\hat{x}_3 = -0.3473$ $\hat{x}_4 = 0.00$, $\hat{x}_5 = 0.3473$, $\hat{x}_6 = 0.7365$ $\hat{x}_7 = 0.8871$	$J(\hat{x}_1) = -4.2717$, $J(\hat{x}_2) = 4.5160$, $J(\hat{x}_3) = -4.2717$ $J(\hat{x}_4) = 9.8696$, $J(\hat{x}_5) = -4.2717$, $J(\hat{x}_6) = 4.5160$ $J(\hat{x}_7) = -4.2717$
2	$\hat{x}_1 = -0.9380$, $\hat{x}_2 = -0.8951$, $\hat{x}_3 = -0.1575$ $\hat{x}_4 = 0.00$, $\hat{x}_5 = 0.1575$, $\hat{x}_6 = 0.8951$ $\hat{x}_7 = 0.9380$	$J(\hat{x}_1) = -6.7258$, $J(\hat{x}_2) = 8.3346$, $J(\hat{x}_3) = -17.1554$ $J(\hat{x}_4) = 19.7392$, $J(\hat{x}_5) = -17.1554$, $J(\hat{x}_6) = 8.3346$ $J(\hat{x}_7) = -6.7258$
⋮	⋮	⋮
Parameter $\tilde{r}$	Enhanced Tent map	
1	$\hat{x}_1 = -0.7365$, $\hat{x}_2 = 0.00$, $\hat{x}_3 = 0.7365$	$J(\hat{x}_1) = -2.1253$, $J(\hat{x}_2) = 3.1416$, $J(\hat{x}_3) = -2.1253$
2	$\hat{x}_1 = -0.4294$, $\hat{x}_2 = 0.00$, $\hat{x}_3 = 0.4294$ $\hat{x}_4 = 0.6030$, $\hat{x}_5 = 0.8410$	$J(\hat{x}_1) = -5.6751$, $J(\hat{x}_2) = 6.2832$, $J(\hat{x}_3) = -5.6751$ $J(\hat{x}_4) = 5.0127$, $J(\hat{x}_5) = -3.4000$
⋮	⋮	⋮

its parameter $\tilde{a} \in [1, 1000]$. As can be observed that the enhanced logistic map has outputs within interval $(-1, 1)$ and these outputs fully distribute in the whole data range. On the other hand, its associated seed map, the logistic map, has frail chaos in only a small parameter range, which can be observed from Fig. 3(b).

B. Enhanced Sine Map

1) Definition: When using SCM to enhance the sine map, namely $F(p, x)$ in (1) is set as the sine map in (12), we can get the enhanced sine map defined as

$$x_{i+1} = \sin(\pi\tilde{\mu}\sin(\pi x_i)) \tag{17}$$

in which $\tilde{\mu}$ is a control parameter and $\tilde{\mu} \in (0, +\infty)$.

2) Fixed Point and Stability: To obtain the fixed points $\hat{x}$ of the enhanced sine map, we set $x_{i+1} = x_i$ and can get the fixed points of the enhanced sine map from the following equation:

$$\hat{x} = \sin(\pi\tilde{\mu}\sin(\pi\hat{x})). \tag{18}$$

Solving the above equation, we can know that $\hat{x} = 0$ is a fixed point of the enhanced sine map in the whole parameter range. When the parameter $\tilde{\mu}$ increases, the enhanced sine map has more fixed points. The derivative of the enhanced sine map can be calculated as

$$J = \frac{dx_{i+1}}{dx_i}$$
$$= \cos(\pi\tilde{\mu}\sin(\pi x_i))\pi\tilde{\mu}\cos(\pi x_i)\pi. \tag{19}$$

Table I lists all the fixed points and their associated derivatives of the enhanced sine map when its parameter $\tilde{\mu} = \{1, 2\}$, and Fig. 2(b) plots the number of fixed points and their minimum absolute derivatives when its parameter $\tilde{\mu} \in [1, 64]$. One can

see that with the parameter increases, the enhanced sine map can obtain more fixed points and all the associated derivatives are without the range $[-1, 1]$, indicating that all its fixed points are unstable.

Fig. 3(c) plots the bifurcation diagram of the enhanced sine map when its parameter $\tilde{\mu} \in [1, 1000]$ and Fig. 3(d) displays the bifurcation diagram of the sine map when its parameter $\mu \in [0, 1]$. One can see that the outputs of the enhanced sine map distribute randomly in the data range $(-1, 1)$, indicating that it can obtain complex dynamics behavior.

C. Enhanced Tent Map

1) Definition: When applying SCM in (1) to the tent map in (13), we can obtain the enhanced tent map defined as

$$x_{i+1} = \begin{cases} \sin(\pi\tilde{r}x_i) & \text{if } x_i < 0.5 \\ \sin(\pi\tilde{r}(1 - x_i)) & \text{if } x_i \geq 0.5 \end{cases} \tag{20}$$

in which $\tilde{r}$ is a parameter and $\tilde{r} \in (0, +\infty)$.

2) Fixed Point and Stability: We can calculate the fixed points of the enhanced tent map from the equation $x_{i+1} = x_i$, namely

$$\hat{x} = \sin(\pi\tilde{r}\min\{\hat{x}, 1 - \hat{x}\}). \tag{21}$$

Obviously, $\hat{x} = 0$ is a fixed point of the enhanced tent map for the parameter $\tilde{r} \in (0, +\infty)$. When $\tilde{r}$ increases, the enhanced tent map has more fixed points. The derivative of the enhanced tent map can be calculated as

$$J = \frac{dx_{i+1}}{dx_i}$$
$$= \begin{cases} \cos(\pi\tilde{r}x_i)\pi\tilde{r} & \text{if } x_i < 0.5 \\ -\cos(\pi\tilde{r}(1 - x_i))\pi\tilde{r} & \text{if } x_i \geq 0.5 \end{cases}. \tag{22}$$
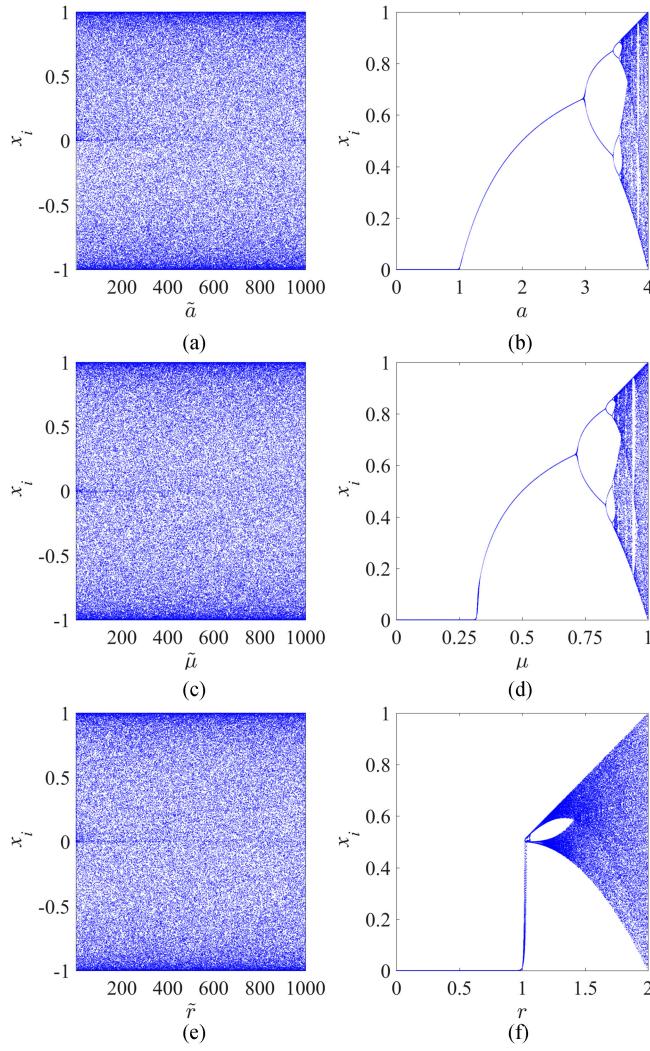
Fig. 3. Bifurcation diagrams of the (a) enhanced logistic map, (b) logistic map, (c) enhanced sine map, (d) sine map, (e) enhanced tent map, and (f) tent map.

Table I lists all the fixed points and their associated derivatives of the enhanced tent map when its parameter $\tilde{r} = \{1, 2\}$. When $\tilde{r} = 1$, the enhanced tent map has three fixed points $\hat{x}_1 = -0.7365$, $\hat{x}_2 = 0$ and $\hat{x}_3 = 0.7365$ and their derivatives are all without interval $[-1, 1]$, which means that they are unstable. Fig. 2(c) plots all the fixed points and their minimum absolute derivatives of the enhanced tent map when its parameter $\tilde{r} \in [1, 64]$. One can observe that all the minimum absolute derivatives are bigger than 1, indicating that all the fixed points are unstable.

Fig. 3(e) plots the bifurcation diagram of the enhanced tent map when its parameter $\tilde{r} \in [1, 1000]$ and Fig. 3(f) shows that of the tent map with its parameter $r \in [0, 2]$. The result shows that the enhanced tent map has much more complex chaotic behavior.

D. Applying SCM to Higher Dimensional Chaotic Map

Besides 1-D chaotic map, the proposed SCM can be used to enhance the chaos complexity of two-dimensional (2-D) or even high-dimensional chaotic maps. In Section II-B, we have used
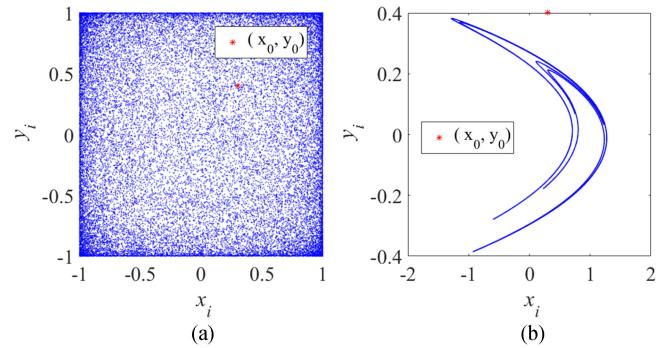

Fig. 4. Trajectories of (a) the enhanced Hénon map with initial point $(x_0, y_0) = (0.3, 0.4)$ and control parameter $(\tilde{a}, \tilde{b}) = (912, 39)$, and (b) the Hénon map with initial point $(x_0, y_0) = (0.3, 0.4)$ and control parameter $(a, b) = (1.4, 0.3)$.

the principle of LE to prove the efficiency of the SCM in 1-D chaotic map. SCM to higher dimensional chaotic maps can also be analyzed using the similar way.

To show the efficiency of the SCM to higher dimensional chaotic maps, we apply SCM to the Hénon map as an example. The Hénon map is a 2-D chaotic map and it is defined as

$$\begin{cases} x_{i+1} = 1 - ax_i^2 + y_i \\ y_{i+1} = bx_i \end{cases} \tag{23}$$

where a and b are two control parameters. When $a = 1.4$ and $b = 0.3$, the Hénon map has chaotic behaviors. When using SCM to enhance the Hénon map, namely setting $F(\cdot)$ in (1) as the Hénon map, the obtained enhanced Hénon map can be obtained as

$$\begin{cases} x_{i+1} = \sin(\pi(1 - \tilde{a}x_i^2 + y_i)) \\ y_{i+1} = \sin(\pi\tilde{b}x_i) \end{cases} \tag{24}$$

where $\tilde{a}$ and $\tilde{b}$ are two control parameters and $\tilde{a}, \tilde{b} \in \mathbb{R}$.

Fig. 4 plots the trajectories of the enhanced Hénon map and the Hénon map. Both initial points are set as $(0.3, 0.4)$. The control parameters of the enhanced Hénon map $(\tilde{a}, \tilde{b})$ are randomly generated, $(912, 39)$ in our experiment, and the control parameter of the Hénon map $(\tilde{a}, \tilde{b})$ are set as $(1.4, 0.3)$, which can make the Hénon map has good chaotic behaviors. One can obverse that the trajectory of the enhanced Hénon map can visit the whole data range in its phase plane and its outputs distribute randomly. On the other hand, the trajectory of the Hénon map can only occupy a very small part in its phase plane. This indicates that the enhanced Hénon map has significantly better complex behaviors than the original Hénon map. Thus, the proposed SCM can efficiently enhance the chaos of the Hénon map.

IV. PERFORMANCE EVALUATIONS

To demonstrate the efficiency of the SCM, this section evaluates the chaos performance of these 1-D enhanced chaotic maps presented in Section III. To show the superiority of the SCM, we compare these enhanced chaotic maps with their seed maps, and new chaotic maps generated by other two methods, namely sine-transform-based chaotic system (STBCS) [42] and chaotic modulation framework (CMF) [30]. The evaluations and com-
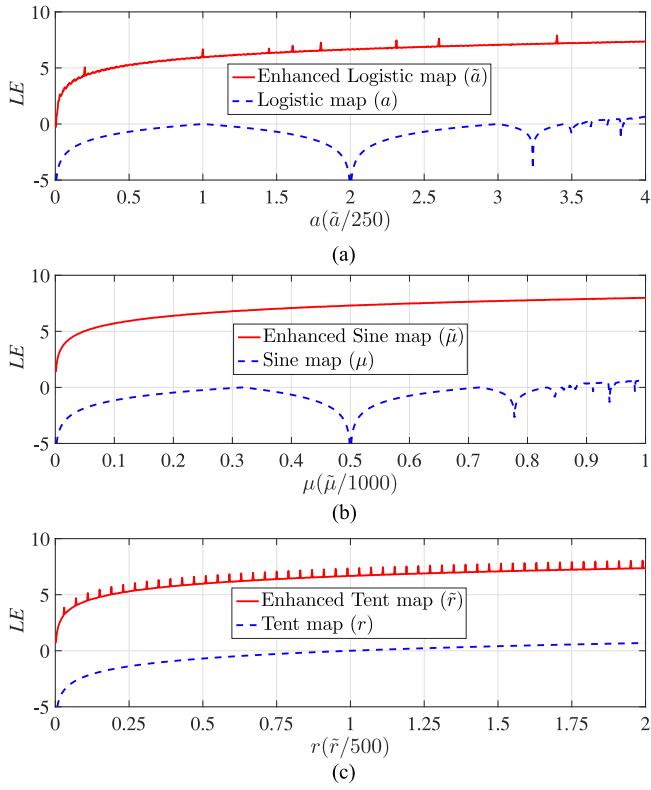
Fig. 5. LE comparisons of (a) the enhanced logistic and logistic maps, (b) the enhanced sine and sine maps, and (c) the enhanced tent and tent maps.

Fig. 6. SE comparisons of different chaotic maps. (a) Enhanced logistic, enhanced sine and enhanced tent maps, and their seed maps. (b) Enhanced logistic, enhanced sine maps, and the LS maps generated by STBCS and CMF. (c) Enhanced logistic, enhanced tent maps, and the LT maps generated by STBCS and CMF. (d) Enhanced tent, enhanced sine maps, and the TS maps generated by STBCS and CMF.

parisons are performed using Lyapunov exponent [43], sample entropy (SE) [44], and correlation dimension (CD) [45].

A. Lyapunov Exponent

From the discussion in Section II-B, the LE can describe the average separation rate of trajectories starting from two extremely close initial states. A positive LE means that a dynamical system's two adjacent trajectories exponentially separate in each iteration and will become different trajectories when the time increases to infinity. Therefore, a dynamical system owning a positive LE is regarded as chaotic and larger LE indicates more complex behavior. Fig. 5 compares the LEs of the enhanced chaotic maps and their associated seed maps. To obtain a straightforward comparison effect, we only plot the LEs of the three enhanced chaotic maps when their parameters are within [1, 1000]. In fact, the three enhanced chaotic maps still have positive LEs when their control parameters increase to a quite large positive number. As can be observed from Fig. 5 that the three enhanced chaotic maps have much larger LEs than their seed maps. With their parameters increase, the LEs of the three enhanced chaotic maps become larger. This proves that SCM can significantly enhance the chaos complexity of existing chaotic maps.

B. Sample Entropy

The SE is a modification of approximate entropy and it assesses the regularity of time-series signal [44]. When using SE

to assess the complexity of the dynamical system, a larger SE means that the output time-series of the system can achieve a lower degree of regularity, and further indicates that the dynamical system has higher complexity.

Fig. 6 plots the SEs of the chaotic maps generated by SCM, STBCS, and CMF and their seed maps. To provide a visualized comparison environment, we linearly scale the parameter ranges of all the chaotic maps as (0, 1). Fig. 6(a) compares the three enhanced chaotic maps by SCM with their seed maps. Figs. 6(b)–(d) compare the SEs of the enhanced chaotic maps by SCM with chaotic maps generated by STBCS and CMF. The proposed SCM is applied to one seed map, while STBCS and CMF need two seed maps to generate a new chaotic map. Then in each comparison, we choose two existing chaotic maps as seed maps. Thus two enhanced chaotic maps can be obtained by SCM, and two new chaotic maps can be generated by STBCS and CMF. From the SE comparisons, we can observe that using the same seed maps, the enhanced chaotic maps obtained by SCM have much larger SEs than the chaotic maps generated by STBCS and CMF in almost all parameter settings. This demonstrates that the enhanced chaotic maps by SCM can generate output time-series with much lower degree of regularity than the chaotic maps generated by the other two methods.

C. Correlation Dimension

The CD is a kind of fractal dimensions and it is designed to test the occupied space dimensionality of a series of points [45]. It can test the strangeness of a chaotic system's chaotic attractor.
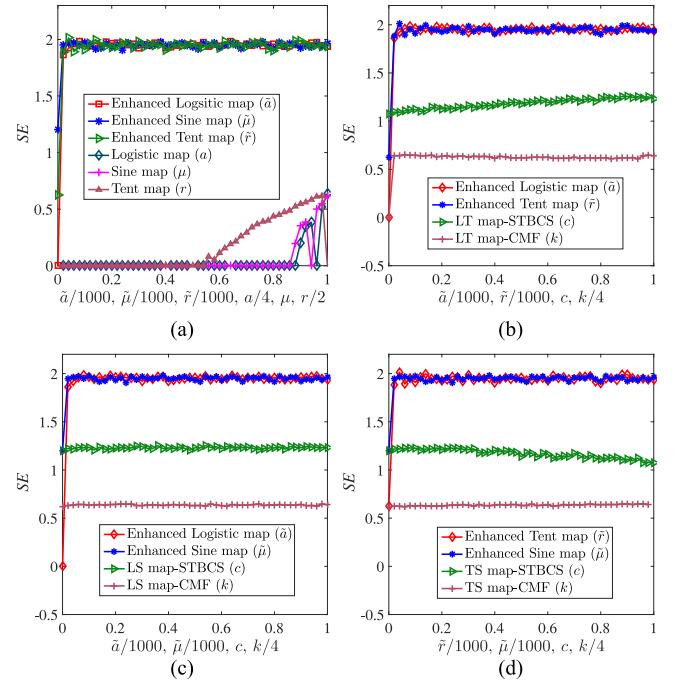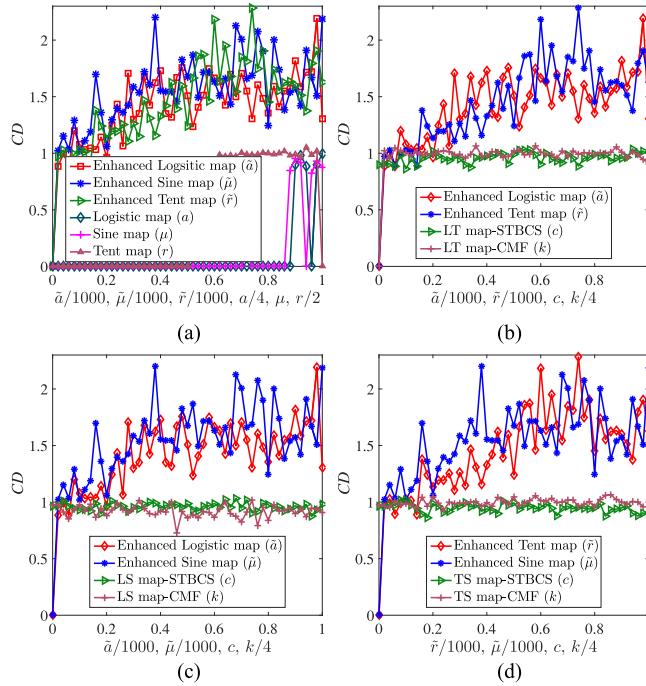
Fig. 7. CD comparisons of different chaotic maps. (a) Enhanced logistic, enhanced sine and enhanced tent maps, and their seed maps. (b) Enhanced logistic, enhanced sine maps, and the LS maps generated by STBCS and CMF. (c) Enhanced logistic, enhanced tent maps, and the LT maps generated by STBCS and CMF. (d) Enhanced tent, enhanced sine maps, and the TS maps generated by STBCS and CMF.

We use the calculation method introduced in [46] to obtain the CDs of different chaotic maps and set the embedding dimension as 2. Fig. 7 plots the CDs of different chaotic maps. Fig. 7(a) compares the CDs of three enhanced chaotic maps with those of their seed maps. It shows that these three enhanced chaotic maps by SCM can achieve much larger positive CDs than their associated seed maps. Figs. 7(b)–(d) compare the CDs of enhanced chaotic maps generated by SCM with those of chaotic maps generated by STBCS and CMF using the same seed maps. One can observe that in most parameter settings, the three enhanced chaotic maps can achieve larger CDs than these chaotic maps generated by STBCS and CMF. This proves that the attractors of the three enhanced chaotic maps are more irregular.

V. HARDWARE IMPLEMENTATION

To show the simple implementation of the proposed SCM, this section designs and tests the circuits of the three enhanced chaotic maps using FPGA.

A. FPGA Structure Setting

The FPGA is a widely used tool to implement the chaotic oscillators. Fig. 8 shows the FPGA structure of the enhanced logistic, enhanced sine and enhanced tent maps. We use the 64-bit double-float data format defined by IEEE 754 standard and the programming language is the very high-speed hardware description language (VHDL). One can see that the whole structure includes four modules: *TxCon*, *TopCon*, *FunCon*,

and *Sin_Pix* modules. The *TxCon* module is a communication control module, which obtains the initial states and parameter settings from the connected computer and sends the iterative results back to the computer. Specially, the variable *RXD* receives the initial states, the parameter *TXD* receives the information that specifies which of the three enhanced chaotic maps is executed, and the parameter *RST* resets the module. The *TopCon* module is the system control module. On one hand, it parses the running parameters and sends these parameters to the function module. On the other hand, it receives the executing results from the function module and returns the results back to the *TxCon* module, and also sends the results to oscilloscope. The *FunCon* module is the function control module, which includes the implementations of the three enhanced chaotic maps using the received variables and sends the iterative results back to the *TopCon* module. The *Sin_Pix* is to implement the sine function $\sin(\pi x)$. It receives parameters from and returns the calculation results back to the *FunCon* module.

B. Implementation Results

Fig. 9 shows the FPGA implementation environment. To compare the hardware implementation results with the software implementation results, we also implement the three enhanced chaotic maps in the software environment using the MATLAB software. The used data format in MATLAB is also the 64-bit double-float format. Fig. 10 plots the simulation results of the enhanced logistic, enhanced sine and enhanced tent maps in both FPGA implementation (hardware environment) and MATLAB implementation (software environment). In each implementation, we use the same initial state and set $(x_0, \tilde{a}/\tilde{\mu}/\tilde{r}) = (-0.842, 2)$ (namely (*BFEAF1A9FBE76C8B*,*4000000000000000*) in FPGA implementation). Because the FPGA outputs are displayed in continuous form in the oscilloscope and the MATLAB outputs are plotted in discrete form, the data curves in FPGA and MATLAB simulations have some visual differences. Actually, the implementation results of the three enhanced chaotic maps are exactly the same in FPGA and MATLAB. This indicates that their implementations own consistency in different platforms, and thus, they are suitable for practical applications.

VI. APPLICATION OF SCM IN PRNG

As chaotic systems have many meaningful properties, such as the initial state sensitivity, ergodicity and unpredictability, they are widely used in designing PRNGs. When chaotic systems are used in PRNGs, their chaos performance dominates the randomness of the PRNGs.

A. Proposed PRNG

When designing chaos-based PRNGs, the chaotic sequences are always directly used as pseudorandom numbers. Here, we also use this strategy to design PRNG. For a chaotic sequence $\{X(i)|i=1,2,\cdots\}$, we convert each of its absolute values to a 52-bit binary stream using IEEE 754 float standard, and obtain $\{X_B(i)|i=1,2,\cdots\}$. Then, the digital numbers from 33rd
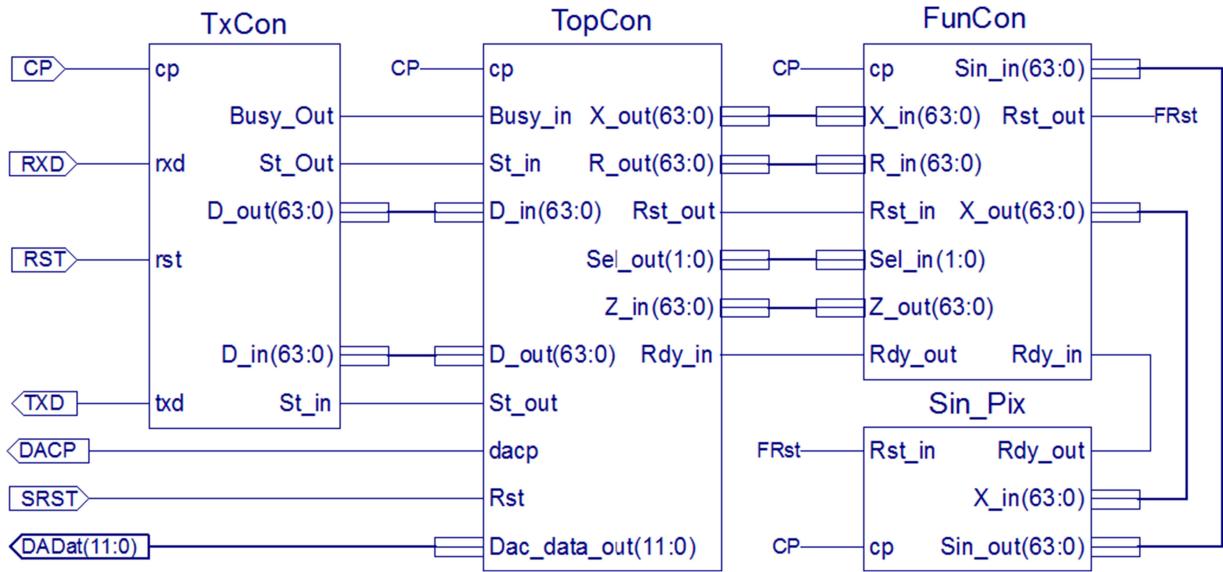
Fig. 8.   FPGA structure of the enhanced logistic, enhanced sine and enhanced tent maps generated by SCM.
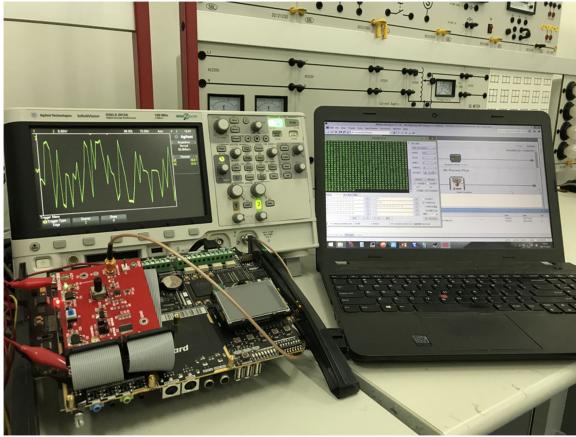

Fig. 9.   Hardware devices of FPGA implementation.

to 40th in each binary stream are used as the pseudorandom numbers. The proposed PRNG can be defined as

$$\text{PRNG} = X_B(i)_{33:40} \qquad (25)$$

It is obvious that each chaotic output can obtain eight binary numbers. The PRNGs using the enhanced logistic, enhanced sine, enhanced tent, logistic, sine and tent maps are called PRNG-ELM, PRNG-ESM, PRNG-ETM, PRNG-LM, PRNG-SM, and PRNG-TM, respectively.

B. Randomness Analysis

Here, we test the randomness of the PRNGs using different chaotic maps.

1) NIST SP800-22: The National Institute of Standards and Technology SP800-22 [47] is a widely used test standard to measure the randomness of random numbers. It includes 15 subtests and each subtest aims to find the nonrandomness area of a random number sequence from different aspects. Each subtest
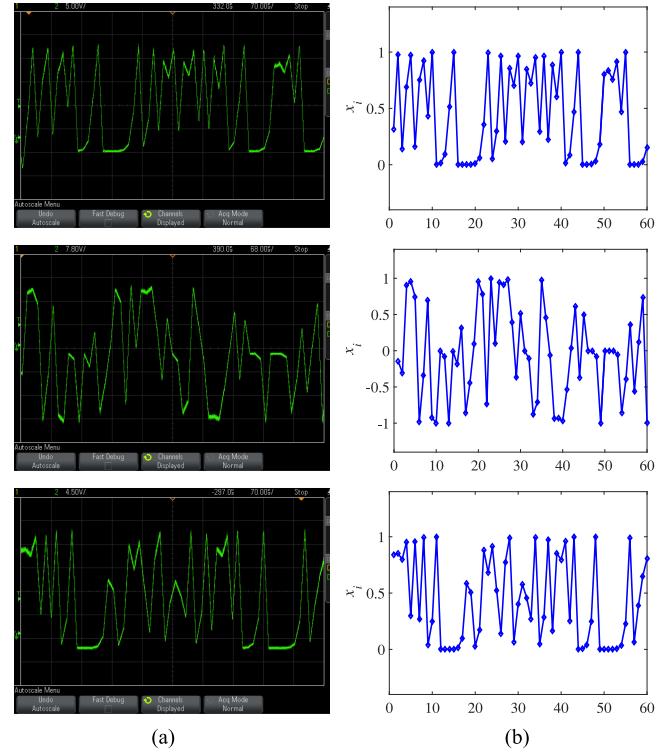

Fig. 10.   Implementation results of the three enhanced chaotic maps. The first, second, and third rows show the first 60 iteration outputs of the enhanced logistic, enhanced sine and enhanced tent maps in (a) FPGA and (b) MATLAB, respectively. Each initial state $(x_0, \tilde{a}/\tilde{\mu}/\tilde{r})$ is set as $(-0.842, 2)$ (namely ($BFEAF1A9FBE76C8B, 4000000000000000$) in FPGA implementation).

will generate a p-value and the random number sequences can pass a sub-test if the corresponding p-value is bigger than the experimental significance level α. The test binary sequence is 1 000 000 bits and the number of sequences should be larger than α^{-1} in one test.

TABLE II
p-VALUE SCORES OF BINARY SEQUENCES GENERATED BY PRNG-ELM, PRNG-ESM, AND PRNG-ETM IN THE NIST SP800-22

Sub-tests	PRNG-ELM	PRNG-ESM	PRNG-ETM
		≥ 0.01	
Frequency	0.654467	0.364146	0.264458
Block Frequency	0.602458	0.437274	0.819544
Cumulative Sums*	0.867206	0.670408	0.358974
Runs	0.834308	0.213309	0.534146
Longest Run	0.862344	0.204076	0.706149
Rank	0.585209	0.819544	0.222869
FFT	0.637119	0.407091	0.568055
Non-Ovla. Temp.*	0.483612	0.472933	0.491181
Ovla. Temp.	0.739918	0.602458	0.186566
Universal	0.407091	0.772760	0.706149
Appr. Entropy	0.772760	0.287306	0.993837
Ran. Exc.*	0.332136	0.442347	0.502979
Ran. Exc. Var.*	0.367181	0.356540	0.534426
Serial*	0.518381	0.175321	0.337793
Linear Complexity	0.671779	0.264458	0.654467
Success Count	15/15	15/15	15/15

*the average values of multiple tests.

TABLE III
TESTU01 RESULTS OF DIFFERENT PRNGS USING DIFFERENT LENGTHS OF RANDOM NUMBERS

PRNGs	*Rabbit*	*Alphabit*
	2^{24} bits	
PRNG-ELM	39/39	17/17
PRNG-ESM	39/39	17/17
PRNG-ETM	39/39	17/17
PRNG-LM	39/39	17/17
PRNG-SM	39/39	17/17
PRNG-TM	27/39	9/17
	2^{28} bits	
PRNG-ELM	40/40	17/17
PRNG-ESM	40/40	17/17
PRNG-ETM	40/40	17/17
PRNG-LM	28/40	8/17
PRNG-SM	31/40	12/17
PRNG-TM	19/40	2/17

According to the recommendation in [47], we set the significance level $\alpha = 0.01$ and use 120 binary sequences with 1 000 000 bits as the testing input. Then, the 120 binary sequences can pass a subtest if the obtained *p*-value is bigger than 0.01. Table II shows the NIST SP800-22 test results of PRNG-ELM, PRNG-ESM, and PRNG-ETM. For each PRNG, we randomly generate 120 binary sequences with 1 000 000 bits as the experimental input. As can be observed that, all the generated *p*-values fall into the range [0.01, 1]. This means that the PRNGs using the three enhanced chaotic maps have high randomness.

2) TestU01: It is also a commonly used test standard for random numbers [48]. It provides a set of utilities for the empirical statistical tests of random numbers. Our experiment uses the two batteries, *Rabbit* and *Alphabit* to test the randomness of different PRNGs. For each PRNG, two binary sequences with 2^{24} bits and 2^{28} bits are tested. The *Rabbit* includes 39 statistical tests for binary sequence with 2^{24} bit, and has 40 statistical tests for binary sequence with 2^{28} bit, while the *Alphabit* applies 17 statistical tests for binary sequence with various lengths.

Table III lists the TestU01 results of different PRNGs using binary sequences with 2^{24} and 2^{28} bits. One can observe that the PRNG-ELM, PRNG-ESM and PRNG-ETM can pass all the statistical tests in the *Rabbit* and *Alphabit*, while the PRNG-LM, PRNG-SM and PRNG-TM fall some tests. This indicates that, using the same strategy, the random numbers generated by the enhanced chaotic maps have better randomness. Thus, the enhanced chaotic maps by SCM have better practicability in the application of PRNG.

VII. CONCLUSION

This paper proposed an SCM to enhance the chaos complexity of existing 1-D chaotic maps. SCM uses a sine function as a nonlinear chaotification transform and can be applied to any existing 1-D chaotic map. We theoretically analyzed the chaos complexity of the SCM using the concept of LE and the analysis result shows that SCM can enhance the chaos complexity of existing chaotic maps in chaotic parameter ranges, and can also produce chaos in nonchaotic parameter ranges. To prove the effect of the SCM, we applied SCM to three 1-D chaotic maps and discussed the chaos dynamics of the generated enhanced chaotic maps. We tested the performance of these enhanced chaotic maps using LE, SE, and CD. The test results show that the enhanced chaotic maps can achieve much wider chaotic regions, and more complex dynamics behaviors than their seed ones. To demonstrate the implementation simplicity of the SCM using hardware device, we implemented the three enhanced chaotic maps using FPGA. PRNGs were further designed using different chaotic maps to show the practical application of the SCM.

REFERENCES

[1] S. Vaidyanathan and C. Volos, *Advances and Applications in Chaotic Systems*. Berlin, Germany: Springer, 2016.
[2] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise: Stochastic Aspects of Dynamics*. vol. 97. Berlin, Germany: Springer, 2013.
[3] H.-J. Stöckmann, *Quantum Chaos: An Introduction*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2007.
[4] S. H. Luo and Y. D. Song, "Chaos analysis-based adaptive backstepping control of the microelectromechanical resonators with constrained output and uncertain time delay," *IEEE Trans. Ind. Electron.*, vol. 63, no. 10, pp. 6217–6225, Oct. 2016.
[5] V. G. Ivancevic and T. T. Ivancevic, *Complex Nonlinearity: Chaos, Phase Transitions, Topology Change and Path Integrals*. Berlin, Germany: Springer, 2008.

[6] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of the generalized discrete Arnold cat map for $N = 2^e$," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 3249–3255, May 2013.

[7] S. Yu, J. Lü, X. Yu, and G. Chen, "Design and implementation of grid multiwing hyperchaotic Lorenz system family via switching control and constructing super-heteroclinic loops," *IEEE Trans. Circuits Syst. I*, vol. 59, no. 5, pp. 1015–1028, May 2012.

[8] Y. Wang, Y. Xia, and P. Zhou, "Fuzzy-model-based sampled-data control of chaotic systems: A fuzzy time-dependent Lyapunov-Krasovskii functional approach," *IEEE Trans. Fuzzy Syst.*, vol. 25, no. 6, pp. 1672–1684, Dec. 2017.

[9] K. Cho and T. Miyano, "Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution," *IEEE Trans. Circuits Syst. I*, vol. 62, no. 2, pp. 478–487, Feb. 2015.

[10] S. H. Strogatz, *Nonlinear Dynamics and Chaos: with Applications to Physics, Biology, Chemistry, and Engineering*. Boulder, CO, USA: Westview, 2014.

[11] H. Bao, N. Wang, B. Bao, M. Chen, P. Jin, and G. Wang, "Initial condition-dependent dynamics and transient period in memristor-based hypogenetic jerk system with four line equilibria," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 57, pp. 264–275, 2018.

[12] B.-C. Bao, Q. Xu, H. Bao, and M. Chen, "Extreme multistability in a memristive circuit," *Electron. Lett.*, vol. 52, no. 12, pp. 1008–1010, 2016.

[13] H. Zhao *et al.*, "Identification of nonlinear dynamic system using a novel recurrent wavelet neural network based on the pipelined architecture," *IEEE Trans. Ind. Electron.*, vol. 61, no. 8, pp. 4171–4182, Aug. 2014.

[14] Y. Zhang and D. Xiao, "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform," *Optics Lasers Eng.*, vol. 51, no. 4, pp. 472–480, 2013.

[15] X. Li, C. Li, and I.-K. Lee, "Chaotic image encryption using pseudo-random masks and pixel mapping," *Signal Process.*, vol. 125, pp. 48–63, 2016.

[16] L. Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 10, pp. 3653–3659, 2014.

[17] Y. Zhang, D. Xiao, Y. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Process., Image Commun.*, vol. 28, no. 3, pp. 292–300, 2013.

[18] S. Chen, S. Yu, J. Lü, G. Chen, and J. He, "Design and FPGA-based realization of a chaotic secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, to be published. doi: 10.1109/TCSVT.2017.2703946.

[19] H.-T. Yau, S.-Y. Wu, C.-L. Chen, and Y.-C. Li, "Fractional-order chaotic self-synchronization-based tracking faults diagnosis of ball bearing systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 6, pp. 3824–3833, Jun. 2016.

[20] G. Li and B. Zhang, "A novel weak signal detection method via chaotic synchronization using Chua's circuit," *IEEE Trans. Ind. Electron.*, vol. 64, no. 3, pp. 2255–2265, Mar. 2017.

[21] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.

[22] R. C. Hilborn, *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, 2nd ed. New York, NY, USA: Oxford Univ. Press, 2001.

[23] J. Lü and G. Chen, "A new chaotic attractor coined," *Int. J. Bifurcation Chaos*, vol. 12, no. 03, pp. 659–661, 2002.

[24] B.-C. Bao, H. Bao, N. Wang, M. Chen, and Q. Xu, "Hidden extreme multistability in memristive hyperchaotic system," *Chaos, Solitons Fractals*, vol. 94, pp. 102–111, 2017.

[25] B. Bao, T. Jiang, G. Wang, P. Jin, H. Bao, and M. Chen, "Two-memristor-based Chuas hyperchaotic circuit with plane equilibrium and its extreme multistability," *Nonlinear Dyn.*, vol. 89, no. 2, pp. 1157–1171, 2017.

[26] C. Shen, S. Yu, J. Lü, and G. Chen, "Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model," *IEEE Trans. Circuits Syst. I*, vol. 61, no. 8, pp. 2380–2389, Aug. 2014.

[27] Y. Deng, H. Hu, W. Xiong, N. N. Xiong, and L. Liu, "Analysis and design of digital chaotic systems with desirable performance via feedback control," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 8, pp. 1187–1200, Aug. 2015.

[28] H. Hu, Y. Xu, and Z. Zhu, "A method of improving the properties of digital chaotic system," *Chaos, Solitons Fractals*, vol. 38, no. 2, pp. 439–446, 2008.

[29] C.-Y. Li, Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, and K. To, "Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG," *IEEE Trans. VLSI Syst.*, vol. 20, no. 2, pp. 385–389, Feb. 2012.

[30] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172–182, 2014.

[31] Q. Wang, S. Yu, C. Li, J. Lu, X. Fang, C. Guyeux, and J. M. Bahi, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I*, vol. 63, no. 3, pp. 401–412, Mar. 2016.

[32] L. Lin, M. Shen, H. C. So, and C. Chang, "Convergence analysis for initial condition estimation in coupled map lattice systems," *IEEE Trans. Signal Process.*, vol. 60, no. 8, pp. 4426–4432, Aug. 2012.

[33] J. A. Lazzús, M. Rivera, and C. H. López-Caraballo, "Parameter estimation of Lorenz chaotic system using a hybrid swarm intelligence algorithm," *Physics Lett. A*, vol. 380, no. 11, pp. 1164–1171, 2016.

[34] D. Li, M. Han, and J. Wang, "Chaotic time series prediction based on a novel robust echo state network," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 23, no. 5, pp. 787–799, May 2012.

[35] M. Liu, S. Zhang, Z. Fan, S. Zheng, and W. Sheng, "Exponential H_∞ synchronization and state estimation for chaotic systems via a unified model," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 24, no. 7, pp. 1114–1126, Jul. 2013.

[36] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," *Image Vis. Comput.*, vol. 27, no. 9, pp. 1371–1381, 2009.

[37] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, and G. Chen, "Cryptanalyzing a chaos-based image encryption algorithm using alternate structure," *J. Syst. Softw.*, vol. 85, no. 9, pp. 2077–2085, 2012.

[38] E. Zeraoulia, *Robust Chaos and Its Applications*. Singapore: World Sci., 2012, vol. 79.

[39] R. Zhang and S. Yang, "Robust chaos synchronization of fractional-order chaotic systems with unknown parameters and uncertain perturbations," *Nonlinear Dyn.*, vol. 69, no. 3, pp. 983–992, 2012.

[40] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016.

[41] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[42] Z. Hua, B. Zhou, and Y. Zhou, "Sine-transform-based chaotic system with FPGA implementation," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2557–2566, Mar. 2018.

[43] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D, Nonlinear Phenom.*, vol. 16, no. 3, pp. 285–317, 1985.

[44] J. S. Richman and J. R. Moorman, "Physiological time-series analysis using approximate entropy and sample entropy," *Amer. J. Physiol.-Heart Circulatory Physiol.*, vol. 278, no. 6, pp. H2039–H2049, 2000.

[45] L. Lacasa and J. Gómez-Gardeñes, "Correlation dimension of complex networks," *Phys. Rev. Lett.*, vol. 110, 2013, Art. no. 168703.

[46] P. Grassberger and I. Procaccia, "Characterization of strange attractors," *Phys. Rev. Lett.*, vol. 50, no. 5, pp. 346–349, 1983.

[47] L. E. B. III *et al.*, "SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Std. Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-22, 2010.

[48] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, no. 4, 2007, Art. no. 22.

Zhongyun Hua (S'14–M'16) received the B.S. degree from Chongqing University, Chongqing, China, in 2011, and the M.S. and Ph.D. degrees from the University of Macau, Macau, China, in 2013 and 2016, respectively, all in software engineering.

He is currently an Associate Professor with the School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China. His research interests include chaotic systems, chaos-based applications, and multimedia security.

Binghang Zhou received the B.S. and M.S. degrees in control engineering from Hunan University, Changsha, China, in 1996 and 2012, respectively.

In 1996, he was an Assistant Engineer with the College of Electrical and Information Engineering, Hunan University, and he has been an Engineer since 2011. His current research interests include embedded system and process control.

Yicong Zhou (M'07–SM'14) received the B.S. degree from Hunan University, Changsha, China in 1992, and the M.S. and Ph.D. degrees from Tufts University, Medford, MA, USA, in 2008 and 2010, respectively, all in electrical engineering.

He is currently an Associate Professor and the Director of the Vision and Image Processing Laboratory, Department of Computer and Information Science, University of Macau, Macau, China. His research interests include chaotic systems, multimedia security, image processing and understanding, and machine learning.

Dr. Zhou was a recipient of the Third Prize of the Macau Natural Science Award in 2014. He is currently a Leading Cochair of the Technical Committee on Cognitive Computing in the IEEE Systems, Man, and Cybernetics Society. He is an Associate Editor for the *Neurocomputing*, *Journal of Visual Communication and Image Representation,* and *Signal Processing: Image Communication.*