Integrated Chaotic Systems for Image Encryption

Rushi Lan, Jinwen He, Shouhua Wang, Tianlong Gu, Xiaonan Luo

PII: S0165-1684(18)30041-0
DOI: 10.1016/j.sigpro.2018.01.026
Reference: SIGPRO 6719

To appear in: *Signal Processing*

Received date: 30 September 2017
Revised date: 25 December 2017
Accepted date: 23 January 2018

Please cite this article as: Rushi Lan, Jinwen He, Shouhua Wang, Tianlong Gu, Xiaonan Luo, Integrated Chaotic Systems for Image Encryption, *Signal Processing* (2018), doi: 10.1016/j.sigpro.2018.01.026

Highlights

- We propose two integrated chaotic systems (ICS) to generate different chaotic maps.
- A new image encryption algorithm is developed using ICS.
- We provide a theoretical study of ICS and extensive security analysis of proposed encryption algorithm.

Integrated Chaotic Systems for Image Encryption

Rushi Lan[a,*], Jinwen He[a,b], Shouhua Wang[b], Tianlong Gu[c], Xiaonan Luo[a]

[a] *Guangxi Colleges and Universities Key Laboratory of Intelligent Processing of Computer Image and Graphics, Guilin University of Electronic Technology, Guilin 541004, China.*
[b] *School of Communication and Information Technology, Guilin University of Electronic Technology, Guilin 541004, China.*
[c] *Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China.*

Abstract

To improve the randomicity behaviors of some existing chaotic maps, this paper proposes two integrated chaotic systems (ICS), which conduct cascade, nonlinear combination, and switch operations to three basic 1D chaotic maps to generate new structures. The developed systems are able to yield several more complicated chaotic maps. Compared with several existing maps, the newly-generated ones have more advanced properties, including wider chaotic ranges, and more complex chaotic behaviors. To demonstrate the effectiveness of ICS, we also design an image encryption scheme based on ICS. Simulation results on different types of images and extensive security analysis demonstrate that the proposed approach has satisfactory properties in image encryption.

Keywords: chaotic maps, image encryption, integrated chaotic systems.

1. Introduction

Chaos theory was first developed in meteorological science by American scientist E.N. Lorenz [1]. As one of the nonlinear dynamics, chaos attracts a huge number of research interests [2, 3], playing many important roles in various fields,

☆This work was supported in part by the National Natural Science Foundation of China (Nos. 61702129, 61772149, and 61320106008), and by Guangxi Colleges and Universities Key Laboratory of Intelligent Processing of Computer Images and Graphics (No. GIIP201703) and Guangxi Key Research and Development Program (Nos. AB17195057 and AB17195025).
*Corresponding author
Email address: rslan2016@163.com (Rushi Lan)

such as science, engineering [4, 5] and economic [6]. More specifically, chaos theory has achieved extremely high application values in electrical engineering [7], e.g., communications [8], random number generators [9], and information security [10, 11, 12].

There are three significant properties of chaotic systems: unpredictability, ergodicity, and initial value sensitivity [13]. Chaotic map is one of the most representative chaotic systems that possesses these properties. Existing chaotic maps can be generally divided into two categories: one dimension (1D) maps and high dimension (HD) maps. For 1D chaotic maps, they have simple structures and are easy to be implemented [14, 15], but they have the defects of limited chaotic ranges [16] and vulnerability [17]. Recently, several novel 1D chaotic maps have been developed gradually such as cascade chaotic system [18], parameter controlling system [19], and nonlinear combination chaotic system [20]. They all expand the range of chaotic maps to acquire better chaotic behaviors. On the other hand, for HD chaotic systems, they have at least two variables, e.g., the Duffing system [21], Clifford system [22], and Hénon system [23]. Compared with 1D chaotic maps, HD chaotic maps have more complex structures and better chaotic behaviors to make their chaotic orbits more unpredictable [24]. Even though, HD chaotic maps have the limitations of high computation cost and implementation difficulty [25].

Image encryption is a hot topic in the fields of image processing and information security. So far, a large number of image encryption algorithms have been developed from different perspectives, such as SCAN [26], circular random grids [27], elliptic curve ElGamal [28], gyrator transform [29], wave transmission [30], visual cryptography [31], fractional Mellin transform [32], p-Fibonacci transform [33], and chaos-based methods. Among these algorithms, the chaos-based encryption approaches are particularly popular thanks to the previously mentioned properties of chaos, which ensure satisfactory encryption performance. Owing to the insecurity of 1D chaotic maps and high computation cost of HD chaotic maps, chaos-based encryption should take account of the advantages of both 1D and HD chaotic maps to design a better chaotic system [34]. To

this end, some recent 1D chaotic maps have complex structures such as cascade chaotic system [18], and nonlinear combination system [20]. However, they still have the limitations of chaotic performance, which will impair encryption effect and make the encrypted images easy to crack. An excellent chaotic system should aggregate the properties of higher complexity and better chaotic performance. It is necessary to design a new chaotic system to overcome the defects referred above.

In this paper, we propose two integrated chaotic systems (ICS) to address the aforementioned limitations of existing 1D and HD chaotic maps. ICS integrates three seed chaotic maps via cascade, nonlinear combination, and switch operations. Setting different seed maps will generate different new chaotic maps. The newly-generated chaotic maps have wider chaotic ranges, higher structure complexity, and acceptable computation cost. We also design a novel image encryption algorithm with the proposed ICS. It is long believed that good chaotic property doesn't necessary lead to a good encryption algorithm [35, 36, 37]. However, ICS based image encryption algorithm has sufficient secret keys, so it has large keyspace and high key sensitivity for image encryption algorithm. The simulation and extensive experimental results show that the ICS is suitable to develop image encryption algorithms.

This paper is an extension of our previous work [38]. In this current paper, we further extend the original framework to a switch-controlled version to acquire more excellent chaotic properties and higher structure complexities. What is more, we also give more in-depth theoretical analyses, more extensive evaluations, and more security analyses on ICS.

The remainder of the paper is organized as follows: Section 2 reviews three traditional chaotic maps. Section 3 introduces the proposed ICS systems, and gives an in-depth analysis of their chaotic properties. Section 4 presents an image encryption algorithm based on ICS. Section 5 and 6 provide extensive experimental results from different perspectives to evaluate the performance of the proposed approach. Section 7 finally reaches a conclusion.

2. Preliminaries

This section briefly reviews three representative chaotic maps, namely Sine map, Tent map, and Logistic map respectively.

2.1. Sine map

Sine map, one of the mostly used 1D chaotic maps, has a simple dynamic structure, but it can generate complex chaotic sequences with a range of [0, 1]. The definition of Sine map is:

$$x_{n+1} = \mathbb{S}(x) = u \sin(\pi x_n), \tag{1}$$

where u is a parameter and $u \in [0, 1]$. The bifurcation diagram and Lyapunov exponent (LE) of Sine map are shown in Fig. 1(a). Note that a positive LE value means the dynamic system is chaotic. From the bifurcation diagram we also can observe that when $u \in [0.87, 1]$, Sine map has a good chaotic behavior.

2.2. Tent map

Tent map is another 1D chaotic map that is used in many applications. It is well known that its graph in bifurcation diagram looks like the curve of tent function. The definition of Tent map is presented as follows,

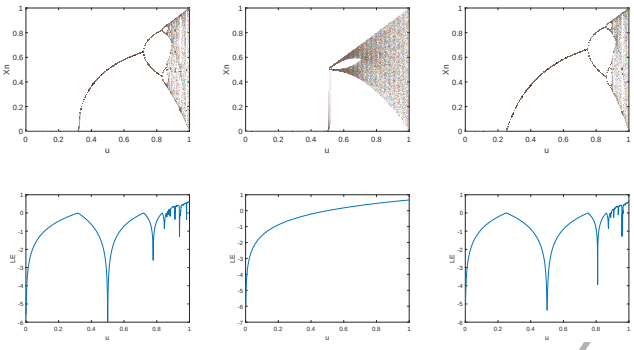
$$x_{n+1} = \mathbb{T}(x) = \begin{cases} 2ux_n & x_n < 0.5, \\ 2u(1 - x_n) & x_n \geq 0.5, \end{cases} \tag{2}$$

where the parameter $u \in [0, 1]$. Fig. 1(b) shows the bifurcation diagram and LE values of Tent map. Obviously, Tent map has a good chaotic behavior when $u \in [0.5, 1]$. In addition, each output sequence has a data range of [0, 1] in this situation.

2.3. Logistic map

Logistic map is derived from Sine map, so they have some similar properties. In order to restrict the input value in a range of [0, 1], Logistic map is mathematically defined as follows:

$$x_{n+1} = \mathbb{L}(x) = 4ux_n(1 - x_n), \tag{3}$$



(a) (b) (c)

Figure 1: Bifurcation diagrams and LE values of three traditional maps. The first row shows bifurcation diagrams of Sine map, Tent map, and Logistic maps respectively. The second row shows their LE values correspondingly.

where the parameter $u \in [0, 1]$. As seen in Fig. 1(c), the graph of Logistic map in bifurcation diagram is similar to that of Sine map. Logistic map has a good chaotic behavior when $u \in [0.9, 1]$.

3. The Proposed ICS

In this section, we detail two developed chaotic systems, denoted by ICS-I and ICS-II, respectively.

3.1. Motivation

Although Sine map, Tent map, and Logistic map are used widely, they have the common defects of limited chaotic ranges. It can be verified in the bifurcation diagrams and LE values plotted in Fig. 1. As can be seen, only partial LE values are larger than 0, indicating that the chaotic behaviors of these maps are restricted according to the property of LE. In addition, the complexities of these maps are simple such that the generated sequences can be predicted easily.

In this work, the proposed ICS is expected to solve the aforementioned defects by integrating some basic maps with different operations. More specif-

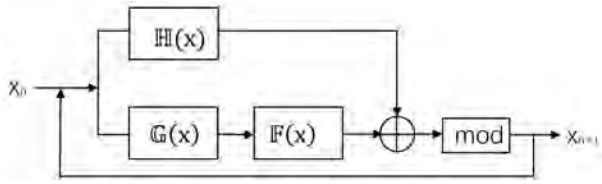


Figure 2: The structure of ICS-I.

ically, cascade operation combines two basic maps like a series circuit, which enhances the complexity of the structure. Meanwhile, nonlinear combination, including addition and modulo operations, is used to extend the chaotic range. To get more favorable chaotic effect, two switches are added in the systems. As a result, ICS becomes more random with the favor of cascade combination, nonlinear operations and switch selection.

3.2. The proposed ICS-I

The structure of ICS-I is illustrated in Fig. 2, where $\mathbb{F}(x)$, $\mathbb{G}(x)$, and $\mathbb{H}(x)$ are three seed chaotic maps. In this paper, Sine map, Tent map, and Logistic map are chosen as seed maps. Mathematically, the proposed ICS-I is defined as follows:

$$x_{n+1} = \tau(x_n) = (\mathbb{F}(\mathbb{G}(x_n)) + \mathbb{H}(x_n)) \mod 1, \tag{4}$$

where x_n is the iteration value, and x_{n+1} is the output of ICS-I. The mod operation here ensures the output is restricted to [0, 1]. Observing Fig. 2 and Eq. (4), ICS-I interates three seed maps by two operations simultaneously. First, the cascade operator is applied to $\mathbb{F}(x)$ and $\mathbb{G}(x)$, which improves complexity level of the chaotic structure. After that, a nonlinear combination opearator, including addition and modulo, is used to $\mathbb{F}(\mathbb{G}(x))$ and $\mathbb{H}(x)$, which strengthens the chaotic behavior with acceptable computation cost and implementation difficulty.

3.3. Chaotic behavior analysis of ICS-I

ICS-I is a dynamic chaotic system with unpredictability and high sensitivity which iterates the cascade chaotic system and seed map nonlinearly, enhancing

Table 1: NEW Chaotic Maps Generated by ICS.

New maps	Definition
LS − S	$x_{n+1} = (4uu\sin(\pi x n)(1-u\sin(\pi x n))+(1-u)\sin(\pi x_n)) \mod 1$
LL − S	$x_{n+1} = (4u(4ux_n(1-x_n))(1-4ux_n(1-x_n))+(1-u)\sin(\pi x_n)) \mod 1$
SL − L	$x_{n+1} = (u\sin(\pi 4ux_n(1-x_n))+(4-4u)x_n(1-x_n)) \mod 1$
SL − T	$x_{n+1} = \begin{cases} (u\sin(\pi 4ux_n(1-x_n))+(2-2u)x_n) \mod 1 & \text{for } x_n < 0.5 \\ (u\sin(\pi 4ux_n(1-x_n))+(2-2u)(1-x_n)) \mod 1 & \text{others} \end{cases}$
LL − T	$x_{n+1} = \begin{cases} (4u(4ux_n(1-x_n))(1-4ux_n(1-x_n))+(2-2u)x_n) \mod 1 & \text{for } x_n < 0.5 \\ (4u(4ux_n(1-x_n))(1-4ux_n(1-x_n))+(2-2u)(1-x_n)) \mod 1 & \text{others} \end{cases}$
LT − S	$x_{n+1} = \begin{cases} (4u(2ux_n)(1-2ux_n)+(1-u)\sin(\pi x_n)) \mod 1 & \text{for } x_n < 0.5 \\ (4u(2u(1-x_n))(1-2u(1-x_n))+(1-u)\sin(\pi x_n)) \mod 1 & \text{others} \end{cases}$
ST − S	$x_{n+1} = \begin{cases} (u\sin(\pi 2ux_n)+(1-u)\sin(\pi x_n)) \mod 1 & \text{for } x_n < 0.5 \\ (u\sin(\pi 2u(1-x_n))+(1-u)\sin(\pi x_n))) \mod 1 & \text{others} \end{cases}$
ST − T	$x_{n+1} = \begin{cases} (u\sin(\pi 2ux_n)+(2-2u)x_n) \mod 1 & \text{for } x_n < 0.5 \\ (u\sin(\pi 2u(1-x_n))+(2-2u)(1-x_n)) \mod 1 & \text{others} \end{cases}$
ST − L	$x_{n+1} = \begin{cases} (u\sin(\pi 2ux_n)+(4-4u)x_n(1-x_n)) \mod 1 & \text{for } x_n < 0.5 \\ (u\sin(\pi 2u(1-x_n))+(4-4u)x_n(1-x_n)) \mod 1 & \text{others} \end{cases}$
LS − T	$x_{n+1} = \begin{cases} (4uu\sin(\pi x_n)(1-u\sin(\pi x_n))+(2-2u)x_n) \mod 1 & \text{for } x_n < 0.5 \\ (4uu\sin(\pi x_n)(1-u\sin(\pi x_n))+(2-2u)(1-x_n)) \mod 1 & \text{others} \end{cases}$
LT − L	$x_{n+1} = \begin{cases} (4u2ux_n(1-2ux_n)+(4-4u)x_n(1-x_n)) \mod 1 & \text{for } x_n < 0.5 \\ (4u2u(1-x_n)(1-2u(1-x_n))+(4-4u)x_n(1-x_n)) \mod 1 & \text{others} \end{cases}$
TT − L	$x_{n+1} = \begin{cases} (2u(2ux_n)+(4-4u)x_n(1-x_n)) \mod 1 & \text{for } x_n < 0.5, 2ux_n < 0.5 \\ (2u(1-2u(2u(1-x_n)))+(4-4u)x_n(1-x_n)) \mod 1 & \text{others} \end{cases}$

the chaotic performances significantly. In this part, we use LE to theoretically study the chaotic behavior of ICS-I. LE denotes the exponential divergence of two extremely close trajectories of a dynamic system. The positive LE value means the two trajectories have totally different exponentially diverge in each unit time. In other words, a system with positive LE values will have a good chaotic behavior.

Assume x_0 and y_0 are two initial values with a small distance of ICS in Eq. (4). x_1 and y_1 are next iteration values of x_0 and y_0. The difference between x_1 and y_1, denoted by $|x_1 - y_1|$, is defined as:

$$|x_1 - y_1| = \left(\frac{|\mathbb{F}(\mathbb{G}(x_0)) - \mathbb{F}(\mathbb{G}(y_0))|}{|\mathbb{G}(x_0) - \mathbb{G}(y_0)|}\frac{|\mathbb{G}(x_0) - \mathbb{G}(y_0)|}{|x_0 - y_0|} + \frac{|\mathbb{H}(x_0) - \mathbb{H}(y_0)|}{|x_0 - y_0|}\right)|x_0 - y_0|. \quad (5)$$

$\mathbb{G}(x_0)$ will be extremely close to $\mathbb{G}(y_0)$ if $x_0 \to y_0$. We can obtain following

results:

$$\left|\frac{d\mathbb{F}}{dx}\mid_{\mathbb{G}(x_0)}\right| \approx \lim_{\mathbb{G}(x_0)\to\mathbb{G}(y_0)} \frac{\left|\mathbb{F}(\mathbb{G}(x_0)) - \mathbb{F}(\mathbb{G}(y_0))\right|}{\left|\mathbb{G}(x_0) - \mathbb{G}(y_0)\right|},$$
$$\left|\frac{d\mathbb{G}}{dx}\mid_{x_0}\right| \approx \lim_{x_0\to y_0} \frac{\left|\mathbb{G}(x_0) - \mathbb{G}(y_0)\right|}{\left|x_0 - y_0\right|},$$
$$\left|\frac{d\mathbb{H}}{dx}\mid_{x_0}\right| \approx \lim_{x_0\to y_0} \frac{\left|\mathbb{H}(x_0) - \mathbb{H}(y_0)\right|}{\left|x_0 - y_0\right|}.$$

Now it has:

$$\left|x_1 - y_1\right| \approx (\left|\frac{d\mathbb{F}}{dx}\mid_{\mathbb{G}(x_0)}\right|\left|\frac{d\mathbb{G}}{dx}\mid_{x_0}\right| + \left|\frac{d\mathbb{H}}{dx}\mid_{x_0}\right|)\left|x_0 - y_0\right|.$$

After n iterations, we can get the following result:

$$\left|x_n - y_n\right| \approx (\left|\prod_{i=0}^{n-1}\frac{d\mathbb{F}}{dx}|_{\mathbb{G}(x_i)}\right|\left|\prod_{i=0}^{n-1}\frac{d\mathbb{G}}{dx}|_{x_i}\right| + \left|\prod_{i=0}^{n-1}\frac{d\mathbb{H}}{dx}|_{x_i}\right|)\left|x_0 - y_0\right|. \tag{6}$$

Then the average change in each iteration from $|x_0 - y_0|$ to $|x_n - y_n|$ is:

$$\Delta\tau(x) \approx \{\left|\prod_{i=0}^{n-1}\frac{d\mathbb{F}}{dx}|_{d\mathbb{G}(x_i)}\right|\left|\prod_{i=0}^{n-1}\frac{d\mathbb{G}}{dx}|_{x_i}\right| + \left|\prod_{i=0}^{n-1}\frac{d\mathbb{H}}{dx}|_{x_i}\right|\}^{\frac{1}{n}}.$$

Accordingly, LE of $\tau(x)$ is calculated as:

$$\lambda_{\tau(x)} = \ln(\Delta\tau(x)) = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln(\left|\frac{d\mathbb{F}}{dx}|_{d\mathbb{G}(x_i)}\right|\left|\frac{d\mathbb{G}}{dx}|_{x_i}\right| + \left|\frac{d\mathbb{H}}{dx}|_{x_i}\right|). \tag{7}$$

Based on the increasing property of $\ln(x)$, it is easy to find that $\Delta\tau(x) \geq \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln(\left|\frac{d\mathbb{F}}{dx}|_{d\mathbb{G}(x_i)}\right|\left|\frac{d\mathbb{G}}{dx}|_{x_i}\right|$. What is more, LEs of $\mathbb{F}(x)$ and $\mathbb{G}(x)$ are defined as :

$$\lambda_{\mathbb{F}(x)} = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln(\left|\frac{d\mathbb{F}}{dx}|_{(x_i)}\right|. \tag{8}$$

$$\lambda_{\mathbb{G}(x)} = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln(\left|\frac{d\mathbb{G}}{dx}|_{(x_i)}\right|. \tag{9}$$

Therefore, we get following result:

$$\lambda_{\tau(x)} \geq \lambda_{\mathbb{F}(x)} + \lambda_{\mathbb{G}(x)}. \tag{10}$$

The larger value of a positive LE indicates the faster divergence of two trajectories and better chaotic performance. From Eq. (10), we also can conclude that ICS-I has more excellent chaotic performance than the chaotic system derived only by cascade operation [18].

3.4. Examples of ICS-I

As aforementioned, ICS-I is able to produce several new chaotic maps. For convenience, we denote the used Sine map, Tent map, and Logistic map by $\mathbb{S}$, $\mathbb{T}$, and $\mathbb{L}$ respectively. Compared with these seed maps, ICS-I possesses more complicated chaotic behaviors, because the chaotic complexity and chaotic range are enhanced in ICS-I. To show the effectiveness of proposed chaotic system, 14 examples of ICS-I are shown in Table 1. We name these produced chaotic maps, by $\mathbb{LT}-\mathbb{S}$, $\mathbb{TL}-\mathbb{S}$, $\mathbb{LT}-\mathbb{L}$, and $\mathbb{TS}-\mathbb{L}$ and so on for short. For example, in $\mathbb{LT}-\mathbb{S}$ system, $\mathbb{LT}$ comprises cascade system Logistic (Tent) and Sine maps, so the $\mathbb{TS}-\mathbb{L}$ system is defined as :

$$x_{n+1} = (\text{Logistic}(\text{Tent}(x_n)) + \text{Sine}(x_n)) \mod 1. \tag{11}$$

We can similarly derive the mathematical formulae of some other generated chaotic maps, which are illustrated in Table 1. Based on the definitions given in Table 1, Fig. 3 illustrates the LE values of some chaotic systems produced by ICS-I. We can find that these chaotic systems have positive LE values in a vast range, which indicates that ICS-I has excellent chaotic behaviors. On the other hand, Fig. 4 also shows the bifurcation diagrams of some generated maps, which have more wider chaotic ranges than their seed maps plotted in Fig. 1. All LE and bifurcation diagram results have testified the advanced performance of ICS-I.

3.5. The proposed ICS-II

To improve the structure complexity and unpredictability of ICS-I, two switches are further added to $\mathbb{F}(x)$ and $\mathbb{H}(x)$ to construct ICS-II. The structure of ICS-II is shown in Fig. 5. Correspondingly, f_n and h_n are set as two control sequences of switches. In this work, f_n and h_n are generated by Sine and Tent maps respectively, and $\mathbb{G}(x)$ is set to Tent map. Control sequence should be different from the sequence used for iteration. The selection criteria is shown as follows:

1. when $f_n < 0.5$, $\mathbb{F}(x)$ is set to be Logistic map, otherwise $\mathbb{F}(x)$ is Tent map.

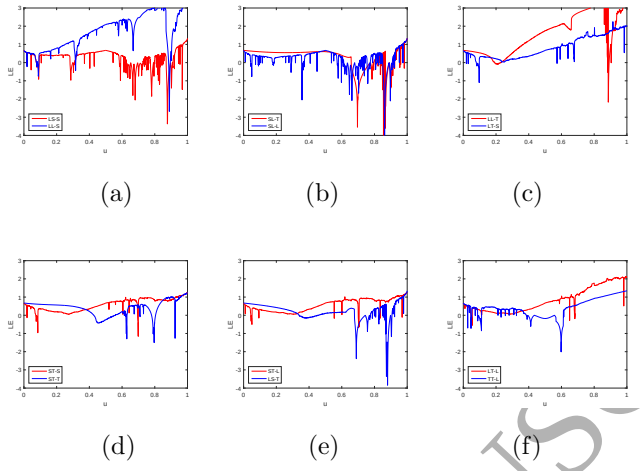


Figure 3: LE values of new chaotic system produced by ICS-I. The first row shows the LE values of $\mathbb{LS}-\mathbb{S}$, $\mathbb{LL}-\mathbb{S}$, $\mathbb{SL}-\mathbb{T}$, $\mathbb{SL}-\mathbb{L}$, $\mathbb{LL}-\mathbb{T}$, and $\mathbb{LT}-\mathbb{S}$. The second row shows those of $\mathbb{ST}-\mathbb{S}$, $\mathbb{ST}-\mathbb{T}$, $\mathbb{ST}-\mathbb{L}$, $\mathbb{LS}-\mathbb{T}$, $\mathbb{LT}-\mathbb{L}$, and $\mathbb{TT}-\mathbb{L}$.

2. when h_n <0.5, $\mathbb{H}(x)$ is set to be Logistic map, otherwise $\mathbb{H}(x)$ is Sine map.

Also, this procedure can be mathematically represented by:

$$x_{n+1} = \begin{cases} \mathbb{F}_1(\mathbb{G}(x_n)) & f_n < 0.5 \\ \mathbb{F}_2(\mathbb{G}(x_n)) & f_n \geq 0.5 \end{cases} + \begin{cases} \mathbb{H}_1(x_n) & h_n < 0.5 \\ \mathbb{H}_2(x_n) & h_n \geq 0.5 \end{cases}, \tag{12}$$

where $\mathbb{F}_1$ and $\mathbb{F}_2$ are Logistic map and Tent map respectively. $\mathbb{H}_1$ is Logistic map, and $\mathbb{H}_2$ is Sine map.

3.6. Discussion

As aforementioned, ICS-I is constructed by performing cascade and nonlinear combination operations to three seed maps synchronously, while ICS-II is derived from ICS-I. Two switches are further added to ICS-I to obtain ICS-II, providing more choices to generate more complicate chaotic sequences. In summary, the proposed two ICS have following flexibilities:

1. combining cascade chaotic system with three seed chaotic maps to form a new chaotic system;

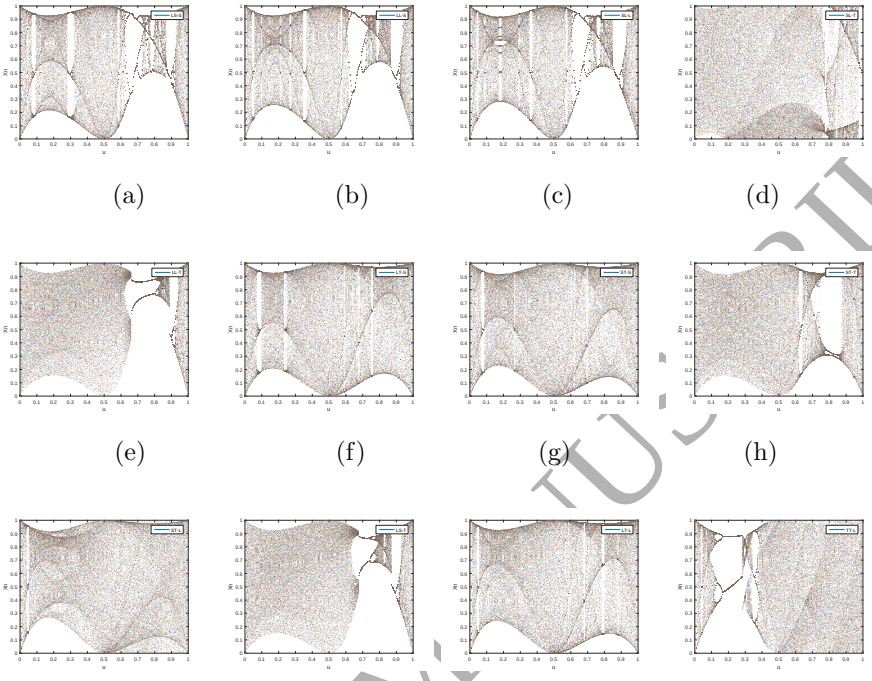


Figure 4: Bifurcation diagrams of (a) $\mathbb{LS}-\mathbb{S}$, (b) $\mathbb{LL}-\mathbb{S}$, (c) $\mathbb{SL}-\mathbb{L}$, (d) $\mathbb{SL}-\mathbb{T}$, (e) $\mathbb{LL}-\mathbb{T}$, (f) $\mathbb{LT}-\mathbb{S}$, (g) $\mathbb{ST}-\mathbb{S}$, (h) $\mathbb{ST}-\mathbb{T}$, (i) $\mathbb{ST}-\mathbb{L}$, (j) $\mathbb{LS}-\mathbb{T}$, (k) $\mathbb{LT}-\mathbb{L}$, and (l) $\mathbb{TT}-\mathbb{L}$.

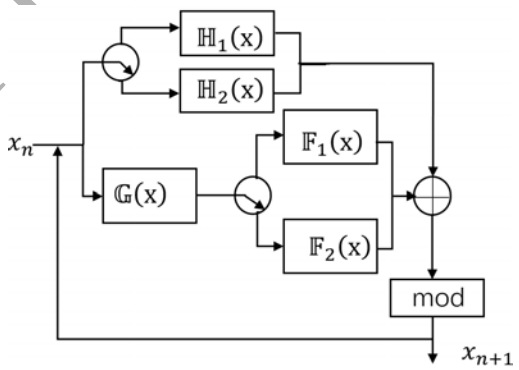


Figure 5: The structure of ICS-II.

2. enhancing the structure complexity of the whole system;
3. achieving a more wider range of chaotic behavior;
4. obtaining the hypersensitivity to its parameters and initial states.

4. Image Encryption

The proposed ICS has excellent chaotic behaviors and high complexity levels, which are suitable for image encryption. This section introduces a new image encryption algorithm named ICS-IE using ICS-II as chaotic sequence generator because it yields more complicated chaotic sequence in every iteration than ICS-I. In the following, we first develop a transform via ICS, named ICST, to disturb the locations and values of pixels in an image, and then detail the derivation of ICS-IE.

4.1. ICST

ICST includes two steps to increase the diffusion and confusion of an image. The first step is to convert the chaotic sequence with a range of [0, 1] into an integer sequence with a range of $[0, N]$. For example, provided that an input chaotic sequence X_i generated by ICS is:

$$X_i=(0.1,\ 0.2,\ 0.3,\ 0.4,\ 0.5,\ 0.6,\ 0.7,\ 0.8,\ 0.9,\ 1).$$

First, X_i is transformed to an integer sequence T_i by $1000 \cdot X_i + 2$. So, the obtained T_i now is:

$$T_i=(102,\ 202,\ 302,\ 402,\ 502,\ 602,\ 702,\ 802,\ 902,\ 1002).$$

Then, T_i is converted to a binary sequence B_i as follows:

$$\begin{gathered}(000001100110,\ 000011001010,\\ 000100101110,\ 000110010010,\\ 000111110100,\ 001001011010,\\ 001010111110,\ 001100100010,\\ 001110000110,\ 001111101010).\end{gathered}$$

Furthermore, B_i will be translated to R_i by exchanging the values of first and seventh positions in every binary number, and R_i is:

(000000100111, 000010001011,
000100101110, 000110010010,
000110110101, 001000011011,
001010111110, 001100100010,
001110000110, 001110101011).

After that, R_i will be transformed to the following integer sequence:

(39, 139, 302, 402, 437, 539, 702, 802, 902, 939).

Finally, the above sequence is conducted a modulo operation with 255, resulting in the ultimate output integer sequence S_i:

S_i=(39, 139, 37, 147, 182, 29, 192, 34, 137, 174).

The first step of ICST is used to change pixel locations of an image. However, it is complex to transform the ICS sequences into integer sequences line by line, so the second transform is proposed to accelerate the process of ICST.

Let I be the original image to be encrypted, and its size is $M \times N$. W_r and W_c are the row and column matrices of I. The process of the second step of ICST includes three steps:

1. There are two sequences T_r and T_c generated by the first transform, and they are with length of M and N respectively,

2. Form row and column matrices according to the following equations:

$$W_c(i,j) = \begin{cases} 1 & \text{for } (T_r(j), j) \\ 0 & \text{others} \end{cases},$$
$$W_r(k,l) = \begin{cases} 1 & \text{for } (k, T_c(k)) \\ 0 & \text{others} \end{cases}, \tag{13}$$

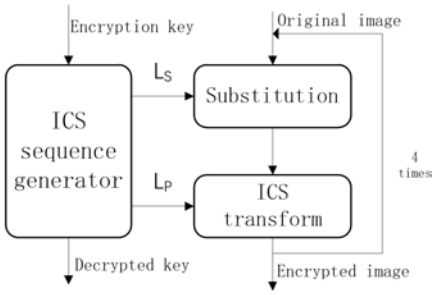


Figure 6: The flowchat of ICS-IE algorithm.

3. Combine the row and column matrices with input image I as follows:

$$S = W_c^T I W_r^T. \tag{14}$$

In the decryption process, the image I will be recovered by the following way:

$$I = (W_c^T)^{-1} S (W_r^T)^{-1}. \tag{15}$$

Note that Eq. (15) is the reverse process of Eq. (14).

ICST is an effective method to change the values and positions of an input image and it can be embeded in many other encryption algorithms. Generally speaking, ICST is an important process in image encryption. The pixel values and positions in an image will get well disturbed after ICST, so that the diffusion and confusion of encrypted image will be significantly enhanced.

4.2. The ICS-based image encryption (ICS-IE) algorithm

This subsection introduces a new image encryption algorithm using ICS-II and ICST. The proposed encryption algorithm is named ICS-IE, which is summarized in Algorithm 1. ICS-IE includes two important procedures: substitution and permutation. The flowchart of the ICS-IE is also shown in Fig. 6. The encryption key k_e consists of f_0, h_0, x_0 and u. In this paper, u is set to be 0.96. f_0, h_0, and x_0 are the initial values of f_n, g_n, and x_n. Moreover, the ICST cycles L times to acquire the best encryption result. The ICST process is

repeated for four times ($L = 4$) to improve the diffusion and confusion properties of encrypted images. So the initial values f_0 and h_0 should be updated for four times according to the following equation:

$$c_0^i = \begin{cases} \frac{1}{2}(c_0 + p) & \text{for } i = 1, \\ \frac{1}{2}(c_0^{i-1} + x_0) & \text{for } i > 1. \end{cases} \tag{16}$$

p is a random number with a range of [0, 1], c_0 represents the initial value, and x_0 is the initial value of a chaotic sequence. f_0 and h_0 get updated with Eq. (16).

Substitution process is used to the encrypted image with the operation shown as follows:

$$E(m,n) = (\lfloor (X_s(k)F) \rfloor - I(m,n)) \mod F, \tag{17}$$

where $\lfloor \cdot \rfloor$ is the floor function. $I(m,n)$ is the input image, and $E(m,n)$ is the output image after substitution process. $X_s(k)$ is the ICS sequence for substitution. In addition, F is the maximal value of $I(m,n)$. m and n are two integers with the ranges of [0, M] and [0, N] respectively.

In image decryption process, the output image $E(m,n)$ will be transformed into input one via the following formula:

$$I(m,n) = (\lfloor (X_s(k)F) \rfloor - E(m,n)) \mod F. \tag{18}$$

The proposed ICST is used in permutation process, which can efficiently change the values and positions of all pixels within the image $E(m,n)$ after substitution process. The diffusion and confusion properties will get remarkable enhanced, because the correlation of the image pixels get well disturbed in the permutation process. Note that image decryption is the inverse process of image encryption. To reconstruct the original image, we can apply the correspondingly inverse transform equations referred in Eq. (15) and Eq. (18).

As mentioned before, substitution and permutation operations are important steps to constitute the ICS-IE algorithm. In summary, ICS-IE has several merits, including

1. possessing higher security levels,
2. havig excellent behaviors in confusion and diffusion aspects,
3. having more choices to set the control parameters, and
4. againsting several attacks, such as data loss, noise and chosen-plaintext.

Algorithm 1 ICS-IE

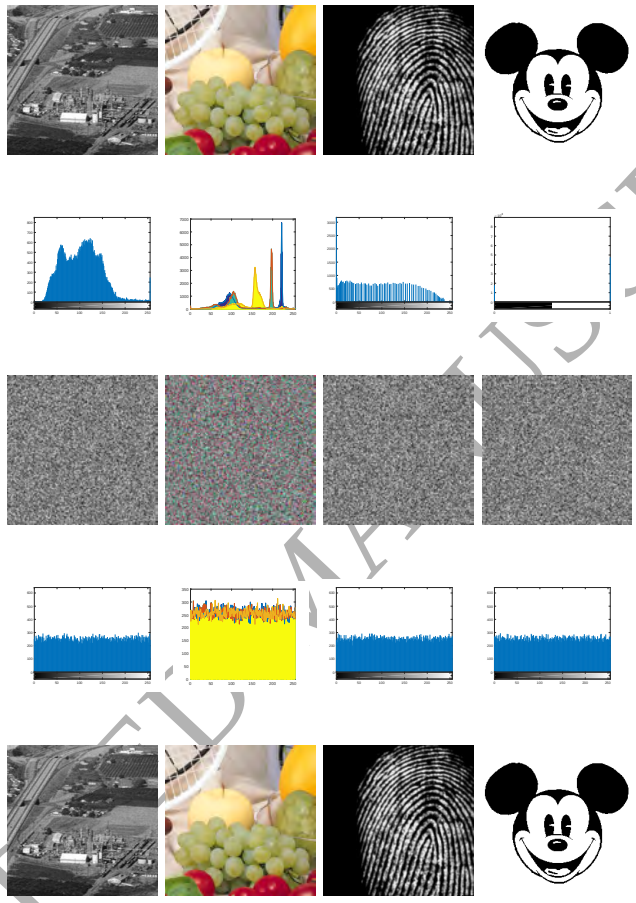
Input: encryption key k_e and original image with size of $M \times N$.

- Step 1: initial the control parameter f_0, h_0, x_0 and u.
- Step 2: For $l = 1$ to L, do
  - **(a)** Generate the ICS sequence X with Eq. (12), the length of X is $L_s + L_p = M \times N + M + N$.
  - **(b)** Conduct substitution operation with the Eq. (17).
  - **(c)** Perform permutation operation with the ICST.

Output: the encrypted image and decryption key.

5. Simulation Results

This section provides encryption and decryption results of the proposed ICS-IE algorithm. As depicted in the first row of Fig. 7, different types of images are considered here, including grayscale image, color image, biometrics image, and binary image, respectively. The simulation results are illustrated in Figs. 7(a)-(d). We can observe that all encrypted images, illustrated on the third row of Fig. 7 are noise-like ciphertext and unrecognized, so that the original information has been well protected. On the other hand, as seen in the second and the fourth rows of Fig. 7, the histograms of encrypted images are uniform-distributed compared with those of the original images that are unevenly distributed. These results indicate that the ICS-IE algorithm performs well in breaking the correlations of image pixels and achieving satisfactory image encryption performance. In addition, the images on the fifth row of Fig. 7 are the corresponding decrypted ones and it can be seen that they all correctly recover to original images.



(a) (b) (c) (d)

Figure 7: Simulation results of different types of images. The first and second rows show original images and their histograms. The third and fourth rows illustrate the ciphertext images and their histograms. The last row shows the decrypted image. The results on the first to fourth columns are corresponding to (a) grayscale image, (b) color image, (c) biometrics image, and (d) binary image respectively.

Table 2: Information Entropy of encrypted images by different schemes.

Filename	*Bao's* [39]	*Liao's* [40]	*Sudoku* [41]	*Zhou's* [42]	*ICS − IE*
5.1.09	7.9966	7.9973	7.9972	7.9971	7.9971
5.1.10	7.9971	7.9973	7.9970	7.9971	7.9971
5.1.11	7.9975	7.9975	7.9974	7.9972	7.9973
5.1.12	7.9972	7.9968	7.9974	7.9970	7.9968
5.1.13	7.9965	7.9976	7.9947	7.9972	7.9974
5.1.14	7.9977	7.9967	7.9970	7.9972	7.9970
5.2.08	7.9991	7.9993	7.9993	7.9993	7.9993
5.2.09	7.9992	7.9993	7.9993	7.9993	7.9993
5.3.01	7.9998	7.9998	7.9998	7.9998	7.9998
5.3.02	7.9996	7.9998	7.9998	7.9998	7.9998
7.1.01	7.9990	7.9993	7.9992	7.9992	7.9992
7.1.02	7.9991	7.9992	7.9990	7.9993	7.9994
7.1.03	7.9990	7.9992	7.9992	7.9992	7.9994
7.1.04	7.9992	7.9993	7.9992	7.9993	7.9992
7.1.05	7.9992	7.9993	7.9992	7.9993	7.9994
7.1.06	7.9992	7.9993	7.9993	7.9993	7.9994
7.1.07	7.9991	7.9993	7.9992	7.9994	7.9993
7.1.08	7.9990	7.9992	7.9991	7.9991	7.9993
7.1.09	7.9991	7.9994	7.9992	7.9994	7.9992
7.1.10	7.9990	7.9993	7.9992	7.9993	7.9993
7.2.01	7.9996	7.9993	7.9997	7.9998	7.9998
Boat.512	7.9992	7.9994	7.9993	7.9994	7.9992
Elaine.512	7.9992	7.9992	7.9992	7.9991	7.9993
Gray21.512	7.9993	7.9992	7.9997	7.9993	7.9994
Numbers.512	7.9994	7.9993	7.9993	7.9993	7.9994
Ruler.512	7.9987	7.9994	7.9995	7.9993	7.9993
Mean	7.998754	7.998846	7.998554	7.998846	**7.998862**

6. Security Analysis

Apart from the encryption results reported in Section 5, security analysis is also a significant aspect to evaluate an encryption algorithm. In this section, we conduct the security analysis of the proposed ICS-IE from different perspectives, namely security key analysis, pixel correlation analysis, information entropy analysis, differential attack, chosen-plaintext attack, noise and data loss attack, and time complexity analysis, respectively. Some commonly used grayscale images are chosen as examples in the following experiments.

6.1. Security key analysis

In the following, we will study the security key from two aspects, i.e., space and sensitivity.

6.1.1. Security key space

It is important for an image encryption algorithm to have a large enough security key space to resist the brute force attacks. For the proposed ICS-IE, the security key includes four parts, namely control parameter u, initial value f_0, h_0, and x_0. Each subkey is in a range of [0, 1]. If the length of every subkey is set to 14 decimals, the key space of ICS-IE will be 10^{56}. As a result, it is large enough to resist brute force attacks.

6.1.2. Key sensitivity analysis

Key sensitivity analysis is usually used to test the ability of resisting inimical deciphering, which detects the variation of encryption results when a slight change (like 10^{-14}) caused in the encryption keys. In this paper, the encryption key k_e is consist of f_0, h_0, x_0 and u. Key sensitivity test is usually tested in the image encryption and decryption procedures as follows: 1) a little change in encryption keys will produce quite different encrypted images; 2) a minor change in decryption keys will result in the failure of recovering image. In addition, the difference between failure reconstruction images is distinct.

The key sensitivity simulation results are shown in Fig. 8. K_1 and K_2 are two encryption keys with a tiny difference of 10^{-14}. Fig. 8(a) is the original image, encrypted respectively with K_1 and K_2 to form Fig. 8(b) and Fig. 8(c). The pixel-to-pixel difference can be acquired by calculating the absolute value of difference between the two encrypted images, which is shown in Fig. 8(d). The corresponding decrypted results with incorrect decryption key K_3 and K_4 are shown in Fig. 8(f) and Fig. 8(g), whose pixel-to-pixel difference is obtained in Fig. 8(h). As can be seen, a tiny difference makes great changes between decrypted images. Therefore, we can conclude that ICS-IE algorithm has a high sensitivity to security keys in both encryption and decryption process. Additionally, only a tiny difference of 10^{-14} can result in significant changes in encryption/decryption results, which means the proposed ICS-IE algorithm has a large key space to defend the inimical deciphering.

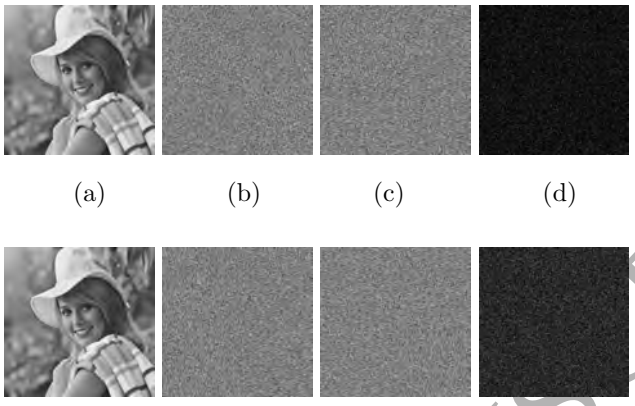


Figure 8: Key sensitivity analysis. (a) Original image. (b) Encryption image C_1 with K_1. (c) Encryption image C_2 with K_2. (d) Difference between encryption images $|C_1\text{-}C_2|$. (e) Decryption image D_1. (f) Decryption image D_2 from C_1 with K_1. (g) Decryption image D_3 from C_1 with K_2. (h) Difference between two encryption images $|D_2\text{-}D_3|$.

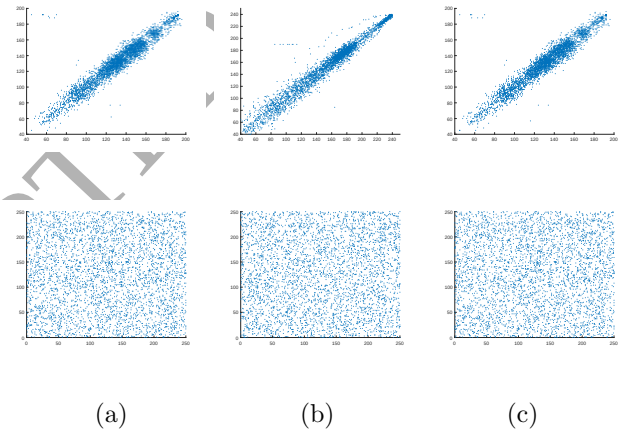


Figure 9: Adjacent pixels correlation of the original and encrypted images at different directions of Fig. 8(a). Top row shows the adjacent pixels correlation of original image at vertical, horizontal and diagonal directions. Correspondingly, bottom row displays the adjacent pixels correlation of original image at the same three directions.

Table 3: Pixel correlation of the original and encrypted images in terms of correlation coefficient.

	Vertival	*Horizontal*	*Diagonal*
Original image	0.9420	0.9455	0.9205
Encrypted image	-2.5×10^{-4}	0.0065	0.0029

6.2. Pixel correlation analysis

In natural images, there are strong correlations of pixels at vertical, horizonal, and diagonal directions. To detect the correlations of adjacent pixels, we randomly select 4000 pixels from the original image as test samples and plot their distributions at three different directions. As shown in the first row of Fig. 9, pixels are distributed near the line $y = x$, which means adjacent pixels have strong correlations. Breaking the high correlation between adjacent pixels is one important step in image encryption. We conduct the same operations to the encrypted images, and the results are plotted in the second row of Fig. 9. It is obviously to see that the adjacent pixels of the encrypted image are distributed uniformly in the whole range.

To specifically calculate the relationship in different directions, the following correlation coefficient is used here:

$$corr(x, y) = \frac{E[(x - \mu_x)(y - \mu_y)]}{\sigma_x \sigma_y}, \tag{19}$$

where x and y are two data sequences, and $E[\cdot]$ is the expectancy function. μ_x and μ_y are mean values of x and y. σ_x and σ_y are the standard deviations. Correlation coefficient is closed to 1 means x and y have a strong correlation. Otherwise, the value is closed to 0 if there is no correlation between x and y. Table 3 shows the comparison of adjacent pixel correlation test between the original image and encrypted image by ICS-IE. It is obviously that the values of pixel correlation are extremely closed to 0, which indicates ICS-IE is able to highly decrease the correlation of pixels in three directions and increase the security level in encryption process.

6.3. Information entropy analysis

Information entropy analysis is a valid way to estimate the randomness of the encrypted images and its definition is given as:

$$H(R) = -\sum_{l=0}^{F-1} P(R = l) \log_2 P(R = l), \tag{20}$$

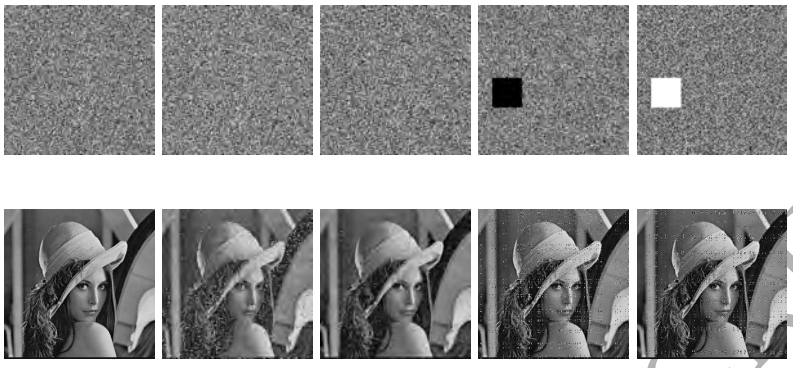
where F is the grayscale level. $P(\cdot)$ is the discrete probability density function to calculate the percentage of pixels.

If the information entropy is close to the maximum value, it means the encrypted image acquires excellent properties of randomness. For a grayscale image, F is an integer with the range of [0, 255]. More specifically, each pixel in gray scale image is represented by 8 binary bits and the expected value of information entropy is 8. As shown in Table 2, 26 experimental images of several different sizes are obtained from the USC-SIPI image database (http://sipi.usc.edu/ database). Information entropy of several encrypted images obtained by different schemes are given. The ICS-IE algorithm achieves the closet average value to 8, which means it posses excellent performance in information entropy. Therefore, the proposed ICS-IE algorithm perfects well in terms of information entropy, which makes the values of encrypted image pixels distribute uniformly with a range of [0, F].

6.4. Differential attack

Differential attack test is another way to measure the encryption performance. An encrypted image can resist the differential attack means it has a good diffusion property. In other word, the differential attack investigates the slight change in input sequence whether influences the output sequence. Number of pixel changing rate (NPCR) and unified average changed intensity (UACI) are two common tools to evaluate differential attack. We give two encrypted images E_1 and E_2 with size of $M \times N$ and their original images only have one bit of pixel difference. L is the gray scale level of the image. For a 8-bit gray scale image, L=256. Mathematically, they are defined as follows:

$$UACI = \frac{1}{MN} \sum_{m=1}^{M} \sum_{n=1}^{N} [\frac{|E_1(m,n) - E_2(m,n)|}{(L-1)}] \times 100, \tag{21}$$



(a) (b) (c) (d) (e)

Figure 10: The images on the first row are the original encrypted images, and its damaged versions by 1% gaussian noise, 5% Salt and Pepper noise, 50*50 square data loss, and 50*50 data loss with a white square , respectively. Those images on the second row are decrypted results of corresponding encrypted images.

and

$$NPCR = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}\varpi(m,n)}{MN} \times 100, \tag{22}$$

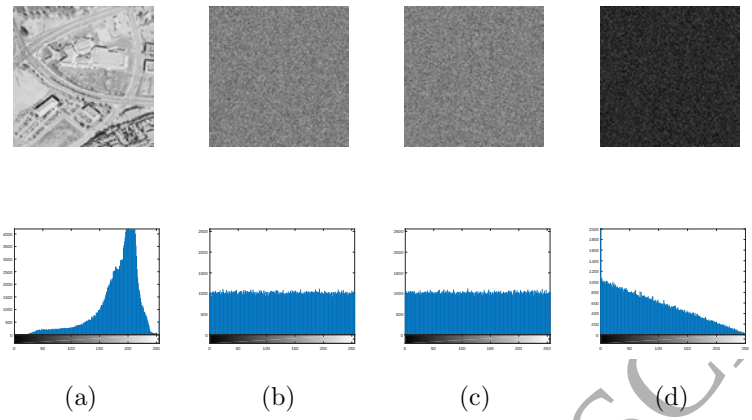
where $\varpi(m,n)=\begin{cases} 1 & \text{for } E_1(m,n) \neq E_2(m,n) \\ 0 & others \end{cases}$. UACI and NPCR both measure the pixel changes between E_1 and E_2. The former one calculates the average value of changed pixels, while the latter one describes the number of changed pixels. For different types of images, the obtained expected values of UACI and NPCR will differ [43]. When the E_1 and E_2 are binary images, the expected values of UACI and NPCR are all 50%, while for 8-bit gray scale image, the expected values respectively are **33.4635**% and **99.6096**%. Table 4 lists the values of UACI and NPCR acquired by several different encryption schemes. As seen in these tables, the scores achieved by ICS-IE algorithm is more closed to their corresponding standard values. These results indicate that ICS-IE has an excellent property of resisting the differential attacks.

6.5. Chosen-plaintext attack

Table 4: UACI/NPCR scores of gray scale images for different image encryption algorithms.

Filename	*Wu's* [19]	*Liao's* [30]	*Hua's* [18]	*Hua's* [42]	*Zhou's*[16]	$ICS-IE$
5.1.09	33.51/99.61	16.67/49.81	33.48/99.60	33.60/99.61	33.14/99.60	33.42/99.60
5.1.10	33.56/99.60	33.54/99.61	33.51/99.61	33.54/99.62	33.24/99.61	33.45/99.64
5.1.11	33.43/99.61	16.70/49.81	33.35/99.61	33.44/99.62	33.72/99.64	33.40/99.61
5.1.12	33.54/99.61	17.06/49.83	33.45/99.63	33.42/99.57	33.56/99.60	33.41/99.60
5.1.13	33.62/99.61	33.64/99.60	33.36/99.59	33.42/99.61	33.77/99.63	33.42/99.59
5.1.14	33.46/99.66	33.30/99.64	33.37/99.67	33.47/99.64	33.21/99.62	33.44/99.63
5.2.08	33.43/99.61	33.43/99.62	33.43/99.60	33.47/99.63	33.31/99.61	33.45/99.62
5.2.09	33.34/99.60	33.46/99.62	33.42/99.60	33.49/99.63	33.62/99.60	33.57/99.63
5.3.01	33.45/99.61	33.81/49.81	33.43/99.61	33.45/99.59	33.42/99.60	33.47/99.61
5.3.02	33.48/99.60	33.62/99.62	33.47/99.61	33.49/99.59	33.29/99.60	33.49/99.61
7.1.01	33.54/99.58	16.82/49.80	33.44/99.61	33.52/99.60	33.25/99.59	33.47/99.59
7.1.02	33.49/99.61	16.81/49.80	33.45/99.60	33.48/99.61	33.53/99.59	33.46/99.62
7.1.03	33.56/99.62	16.73/49.81	33.46/99.59	33.46/99.61	33.27/99.62	33.41/99.62
7.1.04	33.48/99.62	33.48/99.61	33.46/99.62	33.52/99.60	33.21/99.59	33.49/99.59
7.1.05	33.40/99.62	33.46/99.61	33.38/99.59	33.54/99.62	33.21/99.62	33.45/99.60
7.1.06	33.57/99.63	33.45/99.60	33.50/99.60	33.53/99.63	33.30/99.61	33.48/99.61
7.1.07	33.44/99.59	33.52/99.63	33.47/99.59	33.52/99.59	33.15/99.61	33.51/99.63
7.1.08	33.48/99.62	33.45/99.61	33.45/99.61	33.57/99.61	33.26/99.60	33.44/99.59
7.1.09	33.41/99.62	16.77/49.81	33.40/99.61	33.52/99.62	33.23/99.58	33.43/99.61
7.1.10	33.52/99.61	16.86/49.82	33.47/99.61	33.53/99.60	33.59/99.61	33.49/99.60
7.2.01	33.48/99.61	33.47/49.82	33.47/99.62	33.50/99.62	33.42/99.63	33.50/99.61
Elaine.512	33.49/99.58	33.63/99.60	33.52/99.62	33.51/99.62	33.37/99.61	33.51/99.61
Boat.512	33.44/99.61	33.44/99.63	33.38/99.63	33.55/99.62	33.37/99.61	33.47/99.61
Numbers.512	33.54/99.60	33.45/99.61	33.42/99.59	33.40/99.61	33.77/99.61	33.45/99.60
Ruler.512	33.42/99.61	33.06/99.63	33.4/99.62	33.51/99.61	33.43/99.61	33.44/99.59
Gray21.512	33.47/99.62	33.48/99.63	33.40/99.60	33.39/99.60	33.36/99.60	33.50/99.61
Mean	33.4827/99.6104	28.3504/80.4612	33.4362/99.6092	33.4938/99.6100	33.3846/99.6085	**33.4623/99.6095**

The capacity of resisting chosen-plaintext attack is a significant standard to measure security of an image encryption [44, 45, 46]. Some existing algorithms will achieve the same encryption results when they are applied to original images with the same security keys. However, considering the proposed ICS-IE, the initial values are produced randomly, hence our algorithm can generate completely different encrypted images in each iteration even though the algorithm is applied to the same original image with the same set of security keys. As seen in Fig. 11, (a) in top row is original image, and ICS-IE iterates the original images for different times with the same set of security keys. In the top row, Figs. 11(b)-(c) are the encrypted images C_1 and C_2 acquired in the third and fourth iterations respectively, and Fig. 11 (d) shows their pixel-to-pixel difference $|C_1\text{-}C_2|$. In the bottom row of Figs. 11(a)-(d) are histograms of their corresponding images, and the last histogram indicates the C_1 and C_2 are completely different. For an original image with size of $M \times N$, ICS-IE can produce $2^{16(M+N)}$ different encrypted images with the same security keys. In general,



(a) (b) (c) (d)

Figure 11: ICS-IE encrypts an image twice with the same set of security keys. The top row are original image, the encrypted image(C_1) after third encryption run, the encrypted image(C_2) after fourth run and its histogram, and the pixel-to-pixel difference($|C_1\text{-}C_2|$). The bottom row shows their histogram respectively

ICS-IE is able to resist the chosen-plaintext attack.

6.6. Noise and data loss attack

It is inevitable that the digital signal may be corrupted by noise or data loss during the transmission. In this situation, we hope to acquire the content of the original images as much as possible so it is not necessary to transmit the encrypted images again. This experiment investigates the performance of ICS-IE under noise corruption and data loss attack.

Fig. 10(a) shows the encrypted and reconstructed images, and Figs. 10(b)-(c) show the different noise corruptions to image reconstruction. In the top row, the original pictures are added with 1% Gaussian noise and 5% Salt and Pepper noise, then they decrypted with ICS-IE algorithm and the decryption results are shown in the bottom row. As can be seen, although existing some visible noise-like points distribute in reconstruction images, we can see most contents of the original images. In addition, Figs. 10(d)-(e) show the data loss attacks to the encrypted images. In the top row, Fig. 10(d) is randomly cut with a 50×50 patch within the encrypted image, and the pixel values of lost patch are

Table 5: Comparison of time consumption (in second) of different algorithms.

Methods	Zhou's [16]	Zhou's [20]	Hua's [40]	Hua's [42]	ICS-IE
Running Time	0.212321	1.562923	0.540808	81.90322	**0.444224**

all set to 0. Fig. 10(e) has a slight difference with Fig. 10(d) where the pixel values of lost square are set to 255. The corresponding reconstructed images are shown in the bottom row. As can be seen, although there are noise-like points in the reconstructed images, they still preserve most of the visual information and are recognizable. Therefore, ICS-IE algorithm has the capacity of resisting noise corruption and data loss attacks.

6.7. Time complexity analysis

To test the computation cost of different encryption algorithms, we compare the running time of ICS-IE and four representative approaches, namely Zhou's 1D encryption methods [16, 20] and Hua's 2D encryption methods [40, 42]. The experiments here are conducted via MATLAB R2016b in a computer with Windows 10 operation system, Intel(R) Core(TM) i7-6700 CPU @ 3.60GHz and 8GB RAM. All 26 images in the USC SIPI image database, which are used the Section 6.3, are chosen as test images. These images are with different sizes, and they are encrypted with the referred five algorithms. Table 5 shows the average encryption time of these algorithms for one image. It can be seen that speed of ICS-IE is faster than those of two competing 2D encryption algorithms by different degrees. In contrast with two 1D encryption methods, the proposed ICS-IE is faster than the 1D encryption algorithm in [20], but is slower than the one in [16]. The reason lies in that the method in [16] only considers a switch to determine two different chaotic maps, while the proposed one is based on ICS that possesses more complexity chaotic structures. Among all methods, ICS-IE obtains the best encryption performance with a small additional running time.

7. Conclusions

This paper presented ICS-I and ICS-II as two novel structures of chaotic maps. Integrating three seed maps, they are all able to generate several more complicated chaotic maps, which have better chaotic behaviors. We also proposed a novel image encryption algorithm to evaluate the developed chaotic maps. Simulation results and extensive security analysis have shown that ICS-IE algorithm achieved satisfactory performance in image encryption.

8. Acknowledge

The authors would like to sincerely thank the reviewers for their comments and suggestions that significantly improved the quality of this paper.

9. References

References

[1] E. N. Lorenz, Deterministic nonperiodic flow, Journal of the Atmospheric Sciences 20 (2) (1963) 130–141.

[2] H. Dimassi, A. Loria, Adaptive unknown-input observers-based synchronization of chaotic systems for telecommunication, IEEE Transactions on Circuits and Systems I: Regular Papers 58 (4) (2011) 800–812.

[3] Y. Li, G. Chen, W. K.-S. Tang, Controlling a unified chaotic system to hyperchaotic, IEEE Transactions on Circuits and Systems II: Express Briefs 52 (4) (2005) 204–207.

[4] C. Shao, F. Fang, Q. Liu, T. Wang, B. Wang, P. Yin, Recovering chaotic properties from small data, IEEE Transactions on Cybernetics 44 (12) (2014) 2545–2556.

[5] Z.-P. Wang, H.-N. Wu, On fuzzy sampled-data control of chaotic systems via a time-dependent lyapunov functional approach, IEEE Transactions on Cybernetics 45 (4) (2015) 819–829.

[6] C. Kyrtsou, W. C. Labys, Detecting positive feedback in multivariate time series: the case of metal prices and us inflation, Physica A: Statistical Mechanics and Its Applications 377 (1) (2007) 227–229.

[7] S.-L. Chen, T. Hwang, W.-W. Lin, Randomness enhancement using digitalized modified logistic map, IEEE Transactions on Circuits and Systems II: express briefs 57 (12) (2010) 996–1000.

[8] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi, V. Vignoli, A class of maximum-period nonlinear congruential generators derived from the rényi chaotic map, IEEE Transactions on Circuits and Systems I: Regular Papers 54 (4) (2007) 816–828.

[9] Y. Wu, Z. Hua, Y. Zhou, n-dimensional discrete cat map generation using laplace expansions, IEEE Transactions on Cybernetics 46 (11) (2016) 2622–2633.

[10] Y. Wu, Y. Zhou, S. Agaian, J. P. Noonan, A symmetric image cipher using wave perturbations, Signal Processing 102 (2014) 122–131.

[11] Y. Zhou, W. Cao, C. P. Chen, Image encryption using binary bitplane, Signal Processing 100 (2014) 197–207.

[12] R. Bose, S. Pathak, A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system, IEEE Transactions on Circuits and Systems I: Regular Papers 53 (4) (2006) 848–857.

[13] M. R. Frank, L. Mitchell, P. S. Dodds, C. M. Danforth, Standing swells surveyed showing surprisingly stable solutions for the lorenz'96 model, International Journal of Bifurcation and Chaos 24 (10) (2014) 1430027.

[14] X. Wang, L. Teng, X. Qin, A novel color image encryption algorithm based on chaos, Signal Processing 92 (4) (2012) 1101–1108.

[15] G. Bhatnagar, Q. J. Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (4) (2012) 648–663.

[16] Y. Zhou, L. Bao, C. P. Chen, Image encryption using a new parametric switching chaotic system, Signal Processing 93 (11) (2013) 3039–3052.

[17] X. Wu, H. Hu, B. Zhang, Parameter estimation only from the symbolic sequences generated by chaos system, Chaos, Solitons & Fractals 22 (2) (2004) 359–366.

[18] Y. Zhou, Z. Hua, C.-M. Pun, C. P. Chen, Cascade chaotic system with applications, IEEE Transactions on Cybernetics 45 (9) (2015) 2001–2012.

[19] Y. Wu, J. P. Noonan, S. Agaian, A wheel-switch chaotic system for image encryption, in: System Science and Engineering (ICSSE), 2011 International Conference on, IEEE, 2011, pp. 23–27.

[20] Y. Zhou, L. Bao, C. P. Chen, A new 1d chaotic system for image encryption, Signal Processing 97 (2014) 172–182.

[21] I. Kovacic, M. J. Brennan, The Duffing equation: nonlinear oscillators and their behaviour, John Wiley & Sons, 2011.

[22] C. A. Pickover, A note on rendering 3-d strange-attractors, Computers & Graphics 12 (2) (1988) 263–267.

[23] R. C. Hilborn, Chaos and nonlinear dynamics: an introduction for scientists and engineers, Oxford University Press on Demand, 2000.

[24] G. Jakimoski, K. Subbalakshmi, Discrete lyapunov exponent and differential cryptanalysis, IEEE Transactions on Circuits and Systems II: Express Briefs 54 (6) (2007) 499–501.

[25] G. Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognition Letters 31 (5) (2010) 347–354.

[26] R.-J. Chen, S.-J. Horng, Novel scan-ca-based image security system using scan and 2-d von neumann cellular automata, Signal Processing: Image Communication 25 (6) (2010) 413–426.

[27] T.-H. Chen, K.-C. Li, Multi-image encryption by circular random grids, Information Sciences 189 (2012) 255–265.

[28] L. Li, A. A. A. El-Latif, X. Niu, Elliptic curve elgamal based homomorphic image encryption scheme for sharing secret images, Signal Processing 92 (4) (2012) 1069–1078.

[29] Z. Liu, H. Chen, T. Liu, P. Li, L. Xu, J. Dai, S. Liu, Image encryption by using gyrator transform and arnold transform, Journal of Electronic Imaging 20 (1) (2011) 013020–013020.

[30] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Processing 90 (9) (2010) 2714–2722.

[31] T.-H. Chen, K.-H. Tsao, Y.-S. Lee, Yet another multiple-image encryption by rotating random grids, Signal Processing 92 (9) (2012) 2229–2237.

[32] N. Zhou, Y. Wang, L. Gong, Novel optical image encryption scheme based on fractional mellin transform, Optics Communications 284 (13) (2011) 3234–3242.

[33] Y. Zhou, K. Panetta, S. Agaian, C. P. Chen, Image encryption using p-fibonacci transform and decomposition, Optics Communications 285 (5) (2012) 594–608.

[34] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, Chaos: An Interdisciplinary Journal of Nonlinear Science 18 (3) (2008) 033112.

[35] L. Y. Zhang, Y. Zhang, Y. Liu, A. Yang, G. Chen, Security analysis of some diffusion mechanisms used in chaotic ciphers, International Journal of Bifurcation and Chaos 27 (10) (2017) 1750155.

[36] G. ALVAREZ, S. LI, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (08) (2006) 2129–2151.

[37] L. Y. Zhang, Y. Liu, F. Pareschi, Y. Zhang, K.-W. Wong, R. Rovatti, G. Setti, On the security of a class of diffusion mechanisms for image encryption, IEEE Transactions on Cybernetics.

[38] J. He, R. Lan, S. Wang, X. Luo, An integrated chaotic system with application to image encryption, in: 24th International Conferenceon Neural Information Processing, ICONIP 2017, Guangzhou, China, November 14–18, Vol. 10638, Springer, 2017, pp. 837–847.

[39] Y. Zhou, L. Bao, C. P. Chen, Image encryption using a new parametric switching chaotic system, Signal Processing 93 (11) (2013) 3039–3052.

[40] Z. Hua, Y. Zhou, C.-M. Pun, C. P. Chen, 2d sine logistic modulation map for image encryption, Information Sciences 297 (2015) 80–94.

[41] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, P. Natarajan, Local shannon entropy measure with statistical tests for image randomness, Information Sciences 222 (2013) 323–342.

[42] Z. Hua, Y. Zhou, Image encryption using 2d logistic-adjusted-sine map, Information Sciences 339 (2016) 237–253.

[43] C. Fu, J.-j. Chen, H. Zou, W.-h. Meng, Y.-f. Zhan, Y.-w. Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, Optics Express 20 (3) (2012) 2363–2378.

[44] Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, K.-w. Wong, Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure, Nonlinear Dynamics 84 (4) (2016) 2241–2250.

[45] Y. Zhang, D. Xiao, W. Wen, H. Nan, Cryptanalysis of image scrambling based on chaotic sequences and vigenère cipher, Nonlinear Dynamics 78 (1) (2014) 235–240.

[46] L. Y. Zhang, Y. Liu, C. Wang, J. Zhou, Y. Zhang, G. Chen, Improved known-plaintext attack to permutation-only multimedia ciphers, Information Sciences 430 (2018) 228–239.