ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理
Chinese Physics B

# Dynamics analysis of chaotic maps: From perspective on parameter estimation by meta-heuristic algorithm

Yue-Xi Peng(彭越兮), Ke-Hui Sun(孙克辉), Shao-Bo He(贺少波)

**Citation:**Chin. Phys. B . 2020, 29(3): 030502 . **doi:** 10.1088/1674-1056/ab695c
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem

Zeyu Liu(刘泽宇), Tiecheng Xia(夏铁成), Jinbo Wang(王金波)

Chin. Phys. B . 2018, 27(3): 030502 . **doi:** 10.1088/1674-1056/27/3/030502

## Inverse full state hybrid projective synchronizationfor chaotic maps with different dimensions

Adel Ouannas, Giuseppe Grassi

Chin. Phys. B . 2016, 25(9): 090503 . **doi:** 10.1088/1674-1056/25/9/090503

## Chaotic maps and biometrics-based anonymous three-party authenticated key exchange protocol without using passwords

Xie Qi, Hu Bin, Chen Ke-Fei, Liu Wen-Hao, Tan Xiao

Chin. Phys. B . 2015, 24(11): 110505 . **doi:** 10.1088/1674-1056/24/11/110505

## An efficient three-party password-based key agreement protocol using extended chaotic maps

Shu Jian

Chin. Phys. B . 2015, 24(6): 060509 . **doi:** 10.1088/1674-1056/24/6/060509

## Reliability of linear coupling synchronization of hyperchaotic systems with unknown parameters

Li Fan, Wang Chun-Ni, Ma Jun

Chin. Phys. B . 2013, 22(10): 100502 . **doi:** 10.1088/1674-1056/22/10/100502

---

# Dynamics analysis of chaotic maps: From perspective on parameter estimation by meta-heuristic algorithm*

Yue-Xi Peng(彭越兮), Ke-Hui Sun(孙克辉)†, and Shao-Bo He(贺少波)

*School of Physics and Electronics, Central South University, Changsha* 410083, *China*

(Received 6 October 2019; revised manuscript received 26 November 2019; accepted manuscript online 9 January 2020)

Chaotic encryption is one of hot topics in cryptography, which has received increasing attention. Among many encryption methods, chaotic map is employed as an important source of pseudo-random numbers (PRNS). Although the randomness and the butterfly effect of chaotic map make the generated sequence look very confused, its essence is still the deterministic behavior generated by a set of deterministic parameters. Therefore, the unceasing improved parameter estimation technology becomes one of potential threats for chaotic encryption, enhancing the attacking effect of the deciphering methods. In this paper, for better analyzing the cryptography, we focus on investigating the condition of chaotic maps to resist parameter estimation. An improved particle swarm optimization (IPSO) algorithm is introduced as the estimation method. Furthermore, a new piecewise principle is proposed for increasing estimation precision. Detailed experimental results demonstrate the effectiveness of the new estimation principle, and some new requirements are summarized for a secure chaotic encryption system.

**Keywords:** parameter estimation, chaotic map, particle swarm optimization, chaotic encryption

**PACS:** 05.45.Gg, 05.45.Pq **DOI:** 10.1088/1674-1056/ab695c

## 1. Introduction

Over the past twenty years, chaotic secure communication has attracted a lot of attention by the realization of chaotic synchronization.[1] It is widely emerged in engineering applications, such as signal processing,[2–4] speech encryption,[5,6] and image processing.[7–18] In fact, researches on information encryption technology have been studied for several decades, and some classical encryption technologies were proposed, namely the data encryption standard (DES) and the advance encryption standard (AES). However, these traditional encryption methods have some shortcomings, *e.g.*, incapability treating special properties of multimedia data like strong correlation and high redundancy.[19] Especially in the field of image processing, both of the DES and the AES are not suitable for the image encryption.[20] Thus, chaotic encryption becomes a promising encryption technology.

Chaos is characterized in ergodicity, randomness, and initial value sensitivity, which make chaos theory very suitable for cryptography applications. Because the mixing and randomness of chaos are similar to the confusion and diffusion effects in cryptography, chaotic encryption method shows more potential over traditional methods.[21] Compared with continuous-time chaotic systems,[22] chaotic maps are utilized more frequently, featuring its simple structure, no need for solution algorithm and high complexity. Chaotic map is the basis of chaotic cryptography,[23] and it is divided into one-dimensional (1D) and higher-dimensional (HD) cases. For example, Wang *et al.*[11] proposed a row and column switch encryption algorithm based on the classical 1D logistic map. Chenaghlu *et al.*[12] introduced a polynomial combination of 1D chaotic maps in a dynamic image encryption algorithm. To counteract the dynamics degradation of chaotic map in a digital computer as shown in Ref. [24], various enhancing methods for two and higher-dimensional chaotic maps were proposed: two-dimensional (2D) logistic map,[13] three-dimensional (3D) cat map,[14] and hyperchaotic maps[15–18] like 2D sine logistic modulation map (2D-SLMM),[15] 2D-logistic-adjusted-sine map (2D-LASM),[16] 2D sine ICMIC modulation map (2D-SIMM),[17] and 2D logistic ICMIC cascade map (2D-LICM).[18] According to the Kirchhoff criterion: the confidentiality of the system does not depend on the encryption system or the algorithm, but only depend on the key. Hence the parameter estimation technology may become one of threats for chaotic encryption due to its ability to accurately estimate parameters (initial values and system parameters). In contrast, only the equivalent version of PRNS of length as that of known plaintext is recovered in the conventional cryptanalysis methods as shown in Ref. [25]. Therefore, the study of parameter estimation can help people better analyze the chaotic encryption.

Recently, the topics of parameter estimation for chaotic system attracts more and more attention. The meta-heuristic algorithm is one of effective estimation methods,[26–33] featuring good robustness and easy implementation. It converts parameter estimation into an optimization problem, and the

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61161006 and 61573383), the Key Innovation Project of Graduate of Central South University (Grant No. 2018ZZTS009), and the Postdoctoral Innovative Talents Support Program (Grant No. BX20180386).

†Corresponding author. E-mail: kehui@csu.edu.cn

© 2020 Chinese Physical Society and IOP Publishing Ltd 

prior knowledge only takes some pseudo-random sequences generated by chaotic system as the samples. However, because the discrete-time chaotic system has more complex behavior, most of researches on parameter estimation are just limited to estimate the system parameters in continuous-time chaotic system.[26–32] Lately, Du *et al.*[33] successfully identified six continuous-time chaotic systems with unknown initial values and system parameters by a variant differential evolution algorithm. After that, Peng *et al.*[34] investigated the effect of samples on parameter estimation and proposed the IPSO algorithm to estimate parameters of chaotic maps. Simulations demonstrate the better performance of IPSO over other five meta-heuristic algorithms. These studies motivate us to thinking about a new problem: If the initial values and system parameters can be estimated, the secrete key of the chaotic map will be decoded. Therefore, it is interesting to investigate what kind of chaotic map can resist the parameter estimation attack. In addition, because the number of estimated parameters has great influence on estimation results,[34] the precision of traditional estimation principle,[32] *i.e.*, simultaneous estimation of initial values and system parameters, is not high enough. Therefore, we try to propose a new piecewise estimation principle to solve this problem.

The rest of the present article is organized as follows. In Section 2, preliminary knowledge of parameter estimation, namely the traditional principle and the new piecewise parameter estimation principle, are described. The IPSO algorithm is presented in Section 3. Simulation experiments are introduced in Section 4. Finally, we conclude the results and prospects for further researches.

## 2. Parameter estimation of chaotic map

### 2.1. Traditional principle

The traditional parameter estimation for chaotic map is regarded as a multi-dimensional optimization problem. Its principle is illustrated in Fig. 1 and will be described in detail in the following.

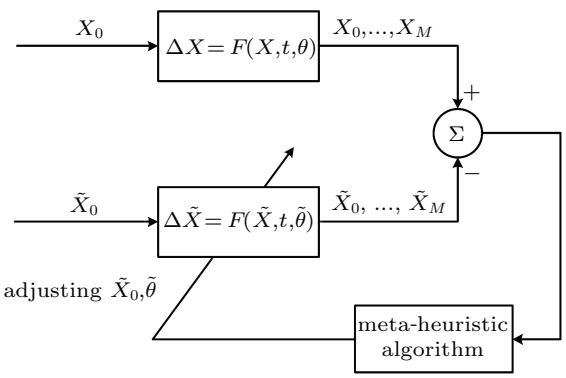



**Fig. 1.** The principle of traditional parameter estimation.

The original chaotic map is described as

$$\Delta X = F(X,t,\theta), \tag{1}$$

where $X = (X_0, X_1, \ldots, X_M)^{\mathrm{T}} \in R^M$ is the $M$-dimensional state vector of the original system ($1 \leq M \leq t$), $t$ is the iteration number of chaotic system, and $X_0$ is the system's initial value, $\theta = (\theta_1, \theta_2, \ldots, \theta_D)^{\mathrm{T}} \in R^D$ denotes the original system parameter and $D$ is the number of estimated system parameter.

Then the estimated system is described by

$$\Delta\tilde{X} = F(\tilde{X},t,\tilde{\theta}), \tag{2}$$

where $\tilde{X} = (\tilde{X}_0, \tilde{X}_1, \ldots, \tilde{X}_M)^{\mathrm{T}} \in R^M$ is the $M$-dimensional state vector of the estimated system, and $M$ is the number of samples. $\tilde{\theta} = (\tilde{\theta}_1, \tilde{\theta}_2, \ldots, \tilde{\theta}_D)^{\mathrm{T}}$ is the estimated system parameter. Finally, the goal of the parameter estimation is defined by

$$J = \frac{1}{M}\sum_{k=1}^{M}(X_k - \tilde{X}_k)^2, \tag{3}$$

where $J$ is the square estimated error, $X_k$ and $\tilde{X}_k$ ($k$=1,2,...,$M$) denote the state at the $k$-th time of the original system and the estimated system, respectively. Essentially, the parameter estimation problem is a multi-dimensional optimization problem with the objective function $J$.

### 2.2. New principle

As shown in Fig. 1, the traditional principle is to adjust the values of $\tilde{X}_0$ and $\tilde{\theta}$ to minimize $J$, that is, the initial values and the system parameters are estimated simultaneously. However, unlike in the continuous-time chaotic system, the chaotic map produces more complex sequence. Too many estimated parameters and initial values may make the estimation process be a complex non-convex optimization problem, resulting in a low estimation precision.

To solve this problem, a new piecewise estimation principle is proposed. The new principle is illustrated in Fig. 2, and it consists of two parts. Here, we divide it into two steps:

**Step 1** In fact, the initial values synchronization of the original system and the estimated system is not a necessary process.[29] Figure 2(a) shows that the initial value $X_l$ of the estimated system is generated by the original system. $l$ is a positive integer ($l \geq 1$), and $X_l, \ldots, X_{l+M}$ is an arbitrary sequence produced by the original system. So, the system parameters are estimated without the constraint of original system initial values.

**Step 2** Based on the accurately estimation of system parameters, then the initial values are estimated.

The new estimation principle corresponds to the piecewise structure of the original principle, and it reduces the difficulty of estimation problem by reducing the considered dimensions.

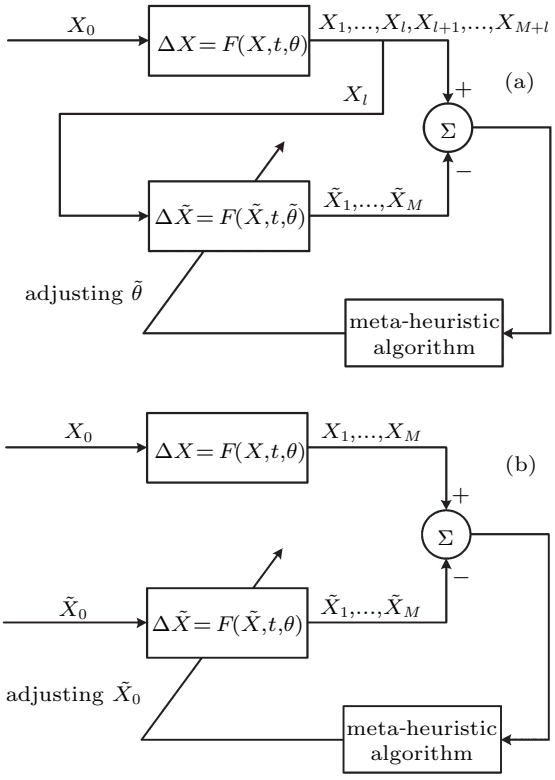



**Fig. 2.** The new principle of parameter estimation: (a) step 1 and (b) step 2.

## 3. IPSO algorithm

The IPSO algorithm separates into the basic PSO algorithm and a special inertia weight. It is specially designed for parameter estimation of chaotic map. Its structure is simple, and the running speed is almost the same as that of the basic PSO algorithm.

### 3.1. Basic PSO algorithm

The PSO algorithm is a well-known meta-heuristic algorithm, which originates the wisdom of bird group.[35] The algorithm describes a process which some particles simulate bird flight in search of food (optimal solution). Each particle represents a bird, and they are initialized with random positions. In each algorithm iteration, particles keep track of its own current optimal and the current population optimal positions to update its velocity, until the optimal solution is found or the termination condition is met. The velocity of particle $i$

$$\begin{aligned} V_i(t+1) &= \omega V_i(t) + c_1 r_1 [J_{bi}(t) - X_i(t)] \\ &\quad + c_2 r_2 [J_g(t) - X_i(t)], \end{aligned} \tag{4}$$

where $V_i(t)$ is the velocity of the particle $i$ at the $t$-th iteration. $\omega$ is called the inertia weight. $c_1$ and $c_2$ are the learning factors. $r_1$ and $r_2$ are random numbers ($r_1, r_2 \in [0,1]$), and they mean that the movement direction of the particle is random. $J_{bi}(t)$ is the optimal position of the particle $i$ at the $t$-th iteration, and $J_g(t)$ represents the population optimal position at the $t$-th iteration. $X_i(t)$ is the position of the particle $i$. In the next iteration, $X_i(t+1)$ is set as

$$X_i(t+1) = X_i(t) + V_i(t+1). \tag{5}$$

The PSO algorithm is divided into global search process and local search process. The global search process refers to the capability of finding the global optimal solution, while the local search process refers to the capability of applying the previous knowledge to find a better solution. The two processes are contradict each other, and the inertia weight $\omega$ is the key to balance them. So, the $\omega$ must be set reasonably to achieve better performance.

In the basic PSO algorithm, inertia weight linearly decreases with increasing iterations. It has been proved that it is not suitable for parameter estimation of chaotic maps,[33] so the special inertia weight in IPSO algorithm is set as

$$\omega(t+1) = (\omega_{\max} - \omega_{\min})\, \mathrm{e}^{-p(t/T)^2} + \omega_{\min}, \tag{6}$$

where $\omega_{\max} = 0.9$ and $\omega_{\min} = 0.4$.[35] $p$ is a constant. $t$ and $T$ are current and maximum iterations of the PSO algorithm, respectively. Without lose of generality, we set $p = 1000$ in this paper.

### 3.2. Implementation of IPSO algorithm in parameter estimation

The implementation steps of the IPSO algorithm are illustrated in Algorithm 1. The encoding of individual particle position in parameter estimation is illustrated in Fig. 3. Part A is the unknown system parameters. Part B is the unknown initial values, and $d$ means the dimension of estimated chaotic map (*i.e.*, $d = 1$ corresponds to 1D chaotic map, $d =$ H corresponds to HD chaotic map).

**Algorithm 1** Pseudo-code of IPSO in parameter estimation.

1. Initialize $N$, $D$, $V_{\max}$, $V_{\min}$, $c_1$, $c_2$, $X(0)$, and $V(0)$
2. Evaluate the fitness value of each particle, find $J_b$ and $J_g$
3. **while** $t < T$ **do**
4. Update $\omega$ by Eq. (6), particle's velocity and position
5. Update particle's velocity and position by Eqs. (4) and (5)
6. Calculate particles' fitness $J(t)$
7. **if** $J(t) < J_b$ **then**
8. $J_b$ is replaced by $J(t)$
9. **end if**
10. **if** $J(t) < J_g$, **then**
11. $J_g$ is replaced by $J(t)$
12. **end if**
13. $t = t + 1$
14. **end while**

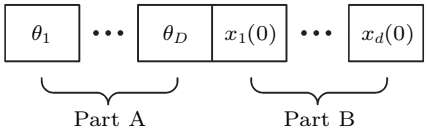



**Fig. 3.** The encoding of individual particle position.

## 4. Numerical simulations

In this section, numerical simulations are carried out in six different chaotic maps, including 2D-logistic map,[13] 2D-LASM,[16] logistic–logistic (LL) map,[36] 2D-SLMM,[15] Chebyshev map (2D),[37] and 2D-LICM.[18] The parameter settings and their corresponding chaotic attractors of these six maps are presented in Table 1 and Fig. 4, respectively. The Lyapunov exponent (LE) is calculated by QR decomposition.[38] In this paper, the $x$-sequence of chaotic map is applied for parameter estimation, so we only calculate the LE of $x$-sequences. Larger LE means more complex chaotic sequence. In general, if the chaotic map with larger LE is applied in secure communication, the security will be better. Simulations are divided into three parts. The first two parts use traditional and new principles to estimate parameters without considering noise. The last part is to estimate parameters by new principle with noise interference.

**Table 2.** Original parameters of different chaotic maps.

| Chaotic map | Parameter settings | LE |
|---|---|---|
| 2D-logistic | $r = 1.190000$, $x(0) = 0.890000$, $y(0) = 0.330000$ | 0.3386 |
| 2D-LASM | $\mu = 0.900000$, $x(0) = 0.100000$, $y(0) = 0.200000$ | 1.0728 |
| LL | $\mu_1 = \mu_2 = 3.900000$, $x(0) = 0.800000$ | 1.0973 |
| 2D-SLMM | $a = 1.000000$, $b = 3.000000$, $x(0) = 0.570000$, $y(0) = 0.620000$ | 0.4604 |
| Chebyshev | $w = 2\pi$, $c = \pi$, $x(0) = 0.500000$, $y(0) = 0.500000$ | 1.8400 |
| 2D-LICM | $a = 3.000000$, $k = 0.800000$, $x(0) = 0.500000$, $y(0) = 0.300000$ | 2.4135 |

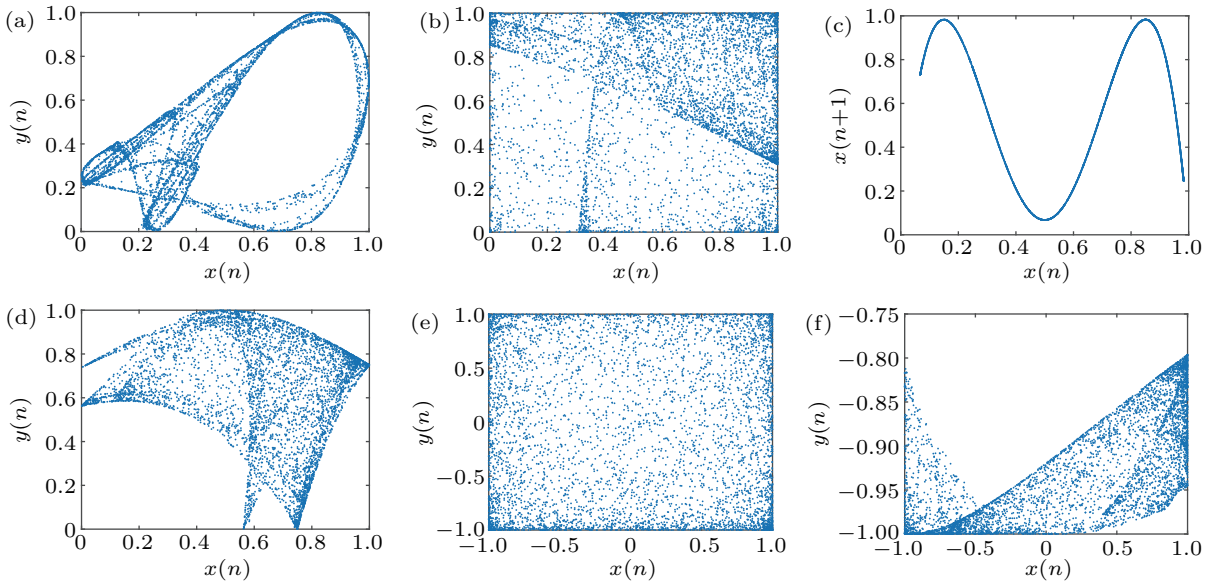



**Fig. 4.** Chaotic attractors based on the parameter settings in Table 1: (a) 2D-logistic map, (b) 2D-LASM, (c) LL map, (d) 2D-SLMM, (e) Chebyshev map, (f) 2D-LICM.

To eliminate the randomness of algorithm and compare the security of chaotic maps, we performed 100 consecutive algorithm runs for each chaotic map. If the error between the final estimation result and the original parameter is less than $1 \times 10^{-6}$, then the estimation is considered to be successful. Here, the success rate is calculated by

$$\text{Success rate} = \frac{\text{successful estimation times}}{100} \times 100\%. \quad (7)$$

The maximum iteration of the IPSO algorithm was set as $T = 300$. According to Ref. [33], the number of samples was set as $M = 2$. The search range for system parameters and initial values are set as [0, 5] and [−1, 1], respectively. Simulations were based on MATLAB 2016a on Intel(R) Core(TM) i5-4200H CPU @2.80 GHz with 4-GB RAM.

### 4.1. Parameter estimation by traditional principle

Parameter estimation results of traditional principle are presented in Table 2. It shows that only the 2D-logistic map and the 2D-LASM were estimated accurately. Because of the smallest number of estimated parameters (three) and the lowest LE (0.3386), the 2D-logistic map has the highest estimated success rate (34%). The estimated success rate of 2D-LASM has dropped a lot to 3% for its much larger LE (1.0728) than that of 2D-logistic map. When the LE is larger, the LL (1.0973) cannot be estimated accurately. Although the LE of 2D-SLMM is only 0.4604, its success rate is 0 for it has four estimated parameters. Because the LE of remaining two chaotic maps is much larger than that of 2D-SLMM, the success rate is still 0.

**Table 2.** Parameter estimation results by traditional principle.

| Chaotic map | Best estimation result | Success rate |
|---|---|---|
| 2D-logistic | $r = 1.190000$, $x(0) = 0.890000$, $y(0) = 0.330000$ | 34% |
| 2D-LASM | $\mu = 0.900000$, $x(0) = 0.100000$, $y(0) = 0.200000$ | 3% |
| LL | $\mu_1 = 3.922757$, $\mu_2 = 3.942643$, $x(0) = 0.801563$ | 0% |
| 2D-SLMM | $a = 0.990127$, $b = 3.034018$, $x(0) = 0.567228$, $y(0) = 0.620939$ | 0% |
| Chebyshev | $w = 6.358846$, $c = 3.155078$, $x(0) = 0.511205$, $y(0) = 0.501639$ | 0% |
| 2D-LICM | $a = 3.687434$, $k = 0.987897$, $x(0) = 0.573314$, $y(0) = 0.889129$ | 0% |

From the above results, it is concluded that: For the traditional estimation principle, if the chaotic map has more than three estimated parameters (including system parameters and initial values) and its LE is larger than that of LL map (1.0973), it is difficult for the general meta-heuristic algorithm to estimate its parameters accurately. Furthermore, the results also demonstrate the conclusions in Ref. [34], *i.e.*, both of the number of estimated parameters and the system complexity affect the estimation precision, and the influence of the estimated number is larger than that of the system complexity.

### 4.2. Parameter estimation by new principle

Parameter estimation results of the new principle are presented in Table 3. From the results of step 1, it shows that the system parameters of all the chaotic maps can be accurately estimated, except for the 2D-LICM with the highest LE (2.4135). The system parameters of 2D-logistic map, 2D-LASM, LL map, and 2D-SLMM are estimated accurately with 100% success rate, but the Chebyshev's success rate drops to 43% for its relatively large LE (1.8400). The process of Step 2 is based on the premise that system parameters have been accurately estimated. Results show that the success rate of the chaotic maps with two estimated parameters (two initial values $x(0)$ and $y(0)$) decreases with the increase of LE, except for LL map that it only has $x$-sequence. Moreover, the initial values of 2D-LICM are accurately estimated with known system parameters, but its success rate is only 1%.

From these results, the conclusions are summarized as: The new principle is more effective than the traditional principle. Based on the new principle, only the 2D-LICM can resist parameter estimation attack. Increasing the number of estimated parameters and LE of chaotic systems is an effective means to increase the resistance to parameter estimation attack, and the influence of the number of estimated parameters is greater than that of LE. In addition, because of the special sensitivity of the initial value for chaotic system, it is more difficult to estimate the initial values than to estimate the system parameters.

**Table 3.** Parameter estimation results by new principle.

| Step | Chaotic map | Best estimation result | Success rate |
|---|---|---|---|
| 1 | 2D-logistic | $r = 1.190000$ | 100% |
| | 2D-LASM | $\mu = 0.900000$ | 100% |
| | LL | $\mu_1 = 3.930000$, $\mu_2 = 3.930000$ | 100% |
| | 2D-SLMM | $a = 1.000000$, $b = 3.000000$ | 100% |
| | Chebyshev | $w = 6.283185$, $c = 3.141593$ | 43% |
| | 2D-LICM | $a = 2.550860$, $k = 1.072577$ | 0% |
| 2 | 2D-logistic | $x(0) = 0.890000$, $y(0) = 0.330000$ | 39% |
| | 2D-LASM | $x(0) = 0.100000$, $y(0) = 0.200000$ | 18% |
| | LL | $x(0) = 0.800000$ | 25% |
| | 2D-SLMM | $x(0) = 0.570000$, $y(0) = 0.620000$ | 23% |
| | Chebyshev | $x(0) = 0.500000$, $y(0) = 0.500000$ | 13% |
| | 2D-LICM | $x(0) = 0.500000$, $y(0) = 0.300000$ | 1% |

### 4.3. Noise interference

Noise is an unavoidable factor in practical applications. Therefore, the parameter estimation of new principle with the the interference of additive white Gaussian noise (AWGN) is considered in this section. In the field of communication, AWGN refers to a kind of noise signal whose spectrum components obey uniform distribution (*i.e.*, white noise) and whose amplitude obeys Gaussian distribution. The noise intensity increases with the decrease of signal-to-noise ratio (SNR).

Here, due to the interference of random noise, it is considered that the estimation is successful if the error is no more than $1 \times 10^{-3}$. Because the 2D-LICM cannot be estimated accurately by the IPSO algorithm, it is not considered in the simulation of this section. Results of step 1 in new estimation principle are presented in Table 4.

**Table 4.** Parameter estimation results by step 1 with noise.

| Chaotic map | 60 dB | | 50 dB | | 40 dB | |
|---|---|---|---|---|---|---|
| | Best estimation result | Success rate | Best estimation result | Success rate | Best estimation result | Success rate |
| 2D-logistic | $r = 1.1900$ | 100% | $r = 1.1900$ | 68% | $r = 1.1900$ | 24% |
| 2D-LASM | $\mu = 0.9000$ | 100% | $\mu = 0.9000$ | 93% | $\mu = 0.9000$ | 32% |
| LL | $\mu_1 = 3.9300$, $\mu_2 = 3.9300$ | 10% | $\mu_1 = 3.9299$, $\mu_2 = 3.9299$ | 5% | $\mu_1 = 3.9334$, $\mu_2 = 3.9307$ | 0% |
| 2D-SLMM | $a = 1.0000$, $b = 3.0000$ | 18% | $a = 1.0000$, $b = 2.9999$ | 3% | $a = 0.9979$, $b = 3.0081$ | 0% |
| Chebyshev | $w = 6.2832$, $c = 3.1412$ | 15% | $w = 6.2831$, $c = 3.1417$ | 2% | $w = 6.2837$, $c = 3.1442$ | 0% |

**Table 5.** Parameter estimation results by step 2 with noise.

| Chaotic map | 60 dB | | 50 dB | | 40 dB | |
|---|---|---|---|---|---|---|
| | Best estimation result | Success rate | Best estimation result | Success rate | Best estimation result | Success rate |
| 2D-logistic | $x(0) = 0.8900$, $y(0) = 0.3300$ | 14% | $x(0) = 0.8901$, $y(0) = 0.3299$ | 2% | $x(0) = 0.8919$, $y(0) = 0.3362$ | 0% |
| 2D-LASM | $x(0) = 0.1000$, $y(0) = 0.2000$ | 8% | $x(0) = 0.1010$, $y(0) = 0.1853$ | 0% | $x(0) = 0.1103$, $y(0) = 0.1627$ | 0% |
| LL | $x(0) = 0.8000$ | 27% | $x(0) = 0.8000$ | 14% | $x(0) = 0.8000$ | 9% |
| 2D-SLMM | $x(0) = 0.5700$, $y(0) = 0.6200$ | 18% | $x(0) = 0.5701$, $y(0) = 0.6201$ | 4% | $x(0) = 0.5721$, $y(0) = 0.6174$ | 0% |
| Chebyshev | $x(0) = 0.5001$, $y(0) = 0.4999$ | 5% | $x(0) = 0.4991$, $y(0) = 0.5008$ | 0% | $x(0) = 0.5207$, $y(0) = 0.5012$ | 0% |

As it is shown, the system parameters of 2D-logistic map and 2D-LASM can still be accurately estimated when the SNR of signal channel reaches 40 dB, but the remaining three maps can only be accurately estimated when the SNR is 50 dB. Results of step 2 are demonstrated in Table 5. When the SNR reaches 40 dB, only the initial values of LL is estimated accurately. Initial values of the 2D-Logistic map and the 2D-SLMM are accurately estimated when the SNR is 50 dB. However, for the 2D-LASM and the Chebyshev map which has higher complexity, they are accurately estimated only when the SNR is raised to 60 dB.

It is concluded that: Under the interference of AWGN, although the estimation precision decreases a lot, most of the chaotic maps are still estimated accurately under the signal with 50-dB SNR. The conclusion in the previous noise-free simulation is valid, that is, chaotic systems with more estimated parameters and larger LE are more difficult to be accurately estimated, and the number of estimated parameters is more influential.

## 5. Conclusion

In this paper, we focus on the dynamics analysis of encryption by chaotic maps, and summarized some new requirements for the secure chaotic encryption system. The IPSO algorithm is introduced for parameter estimation of chaotic maps, and a new piecewise estimation principle is proposed. Numerical simulations were carried out in six different chaotic maps with unknown system parameters and initial values, and the results lead to the following conclusions.

(i) The design of chaotic maps with more estimated parameters and larger LE is more effective against the estimation attack. From the results in this paper, it is more important to increase the number of system parameters and initial values (the component of secrete key) than to enhance the LE of the chaotic system.

(ii) The new piecewise parameter estimation principle is more effective than the traditional one.

(iii) In our simulations, utilizing the 2D-LICM (4 estimated parameters and LE: 2.4135) for chaotic encryption is the relatively secure method.

(v) Estimating initial values are more difficult than estimating system parameters.

In the simulations, some practical factors are considered, including unknown system parameters, unknown initial values, and noise interference. These simulations were therefore theoretically constitute a possibility of anti-chaotic encryption. In the future, more powerful meta-heuristic algorithms may be proposed by the efforts of researchers, so how to construct a chaotic system with both simple structure and high complexity is a problem worthy of continuously concerned. What is more important is that the introduced approach may be a useful tool for the cryptanalysis and the synchronization of chaotic maps. Our next work is to use this method in the applications of chaotic secure communication.

## References


[1] Pecora L and Carroll T 1990 *Phys. Rev. Lett.* **64** 821
[2] Zhang Z, Feng X, Yao Z, *et al*. 2015 *Chin. Phys. B* **24** 110503
[3] Roy A and Misra A 2017 *Euro. Phys. J. Plus* **132** 524
[4] Altaf M, Ahmad A, Khan F, *et al*. 2017 *Multimed. Tools Appl.* **77** 27981
[5] Azzaz M, Tanougast C, Sadoudi S, *et al*. 2013 *Commun. Nonlinear Sci.* **18** 2035
[6] Sheu L 2011 *Nonlinear Dyn.* **1–2** 103
[7] Liu Z, Xia T and Wang J 2018 *Chin. Phys. B* **27** 030502
[8] Chen Y, Wang J, Chen X, *et al*. 2019 *IEEE Access* **7** 58791
[9] Cheng G, Wang C and Chen H, *et al*. 2019 *Int. J. Bifur. Chaos* **29** 1950115
[10] Yin Q and Wang C 2018 *Int. J. Bifur. Chaos* **28** 1850047
[11] Wang X, Wang Q and Zhang Y 2015 *Nonlinear Dyn.* **79** 1141
[12] Asgari-Chenaghlu M, Balafar M A and Feizi-Derakhshi M R 2019 *Signal Process.* **57** 1
[13] Wu Y, Noonan J, Yang G, *et al*. 2012 *J. Electron. Imaging* **21** 013014
[14] Xie Y, Li J, Kong Z, *et al*. 2016 *J. Lightwave Technol.* **34** 5101
[15] Hua Z, Zhou Y, Pun C M, *et al*. 2015 *Inform. Sci.* **297** 80
[16] Hua Z and Zhou Y 2016 *Inform. Sci.* **339** 237
[17] Liu W, Sun K and Zhu C 2016 *Opt. Laser Eng.* **84** 26
[18] Cao C, Sun K and Liu W 2018 *Signal Process.* **143** 122
[19] Nepomuceno E, Nardo L, Arias-Garcia J, *et al*. 2019 *Chaos* **29** 061101
[20] Li C, Lin D, Lü J, *et al*. 2018 *IEEE T. Multimedia* **25** 46
[21] Mao Y and Chen G 2005 *Chaos-Based Image Encryption* (Berlin: Springer)

[22] Wang N, Li C, Bao H, *et al.* 2019 *IEEE T. Circuit-I* **66** 4767
[23] Hua Z, Zhou Y and Bao B 2019 *IEEE T. Ind. Inform.* **480** 403
[24] Li C, Feng B, Li S, *et al*. 2019 *IEEE T. Circuit-I* **66** 2322
[25] Li C, Lin D, Feng B, *et al*. 2018 *IEEE Access* **6** 75834
[26] Peng H, Li L, Yang Y, *et al*. 2010 *Phys. Rev. E* **81** 016207
[27] Zheng S, Wang J, Zhou S, *et al*. 2014 *Chaos* **24** 013133
[28] Lazzús J, Rivera M and López-Caraballo C 2016 *Phys. Lett. A* **380** 1164
[29] Peng Y, Sun K, He S, *et al*. 2018 *Eur. Phys. J. Plus* **133** 305
[30] Xu S, Wang Y and Liu X 2018 *Neural Comput. Appl.* **30** 2607
[31] Yousri D, AbdelAty A, Said L, *et al*. 2019 *Nonlinear Dyn.* **95** 2491
[32] Du W, Miao Q, Tong L, *et al*. 2017 *Phys. Lett. A* **381** 1943
[33] Peng Y, Sun K, He S, *et al*. 2019 *Entropy* **21** 27
[34] Peng Y, Sun K, He S, *et al*. 2019 *Mod. Phys. Lett. B* **33** 1950041
[35] Wang D, Tan D and Liu L 2018 *Soft Comput.* **22** 387
[36] Wang G and Yuan F 2013 *Acta Phys. Sin.* **62** 020506 (in Chinese)
[37] Lee T F 2018 *IEEE Syst. J.* **12** 1499
[38] Ginelli F, Poggi P, Turchi A, *et al*. 2007 *Phys. Rev. Lett.* **99** 130601