IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 July 2023, accepted 31 July 2023, date of publication 4 August 2023, date of current version 11 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3302012

RESEARCH ARTICLE

Second-Order Chaotic Maps With Random Coefficients to Generate Complex Chaotic Sequences for High-Security Image Encryption

TA-CHIEN YEH AND JEAN-FU KIANG, (Life Senior Member, IEEE)
Graduate Institute of Communication Engineering, National Taiwan University, Taipei 10617, Taiwan
Corresponding author: Jean-Fu Kiang (jfkiang@ntu.edu.tw)

ABSTRACT Chaotic maps have been widely applied on image encryption for their complexity and sensitivity to key variation. In this work, we propose second-order chaotic maps with optimized random coefficients to generate chaotic sequences for image encryption. Two screening conditions are proposed to identify 300 candidate chaotic maps in terms of complexity indices K and spectral entropy (SE). A particle swarm optimization algorithm is developed to search for the optimal chaotic maps under eight different weighting schemes. The optimal chaotic maps can achieve $N_p = 2$, $D_{KY} = 2$, CD $= 2$, $K > 0.9$, SE > 0.9 and PE > 0.7. Key sensitivity analysis on all the system parameters and initial values confirms high security of the optimal chaotic maps. A hybrid sequence generation (HSG) scheme is also proposed to further reduce the image encryption time.

INDEX TERMS Image encryption, chaotic map, chaotic sequence, key sensitivity.

I. INTRODUCTION

A chaotic map of dimension N can be characterized with N first-order difference equations as $x_n[\ell+1] = f_n(x_n[\ell])$, with $n = 1, 2, \cdots, N$ [1]. The generated N sequences can be represented as $\bar{x}[\ell] = (x_1[\ell], x_2[\ell], \cdots, x_N[\ell])$ in an N-dimensional phase space. The functional form of f_n can be tuned with a few system parameters to manifest chaotic trace of $\bar{x}[\ell]$ in the phase space as ℓ marches on [2].

A small perturbation to the initial value $\bar{x}[1]$ of a chaotic map usually results in a very different trace in the phase space. Most chaotic systems manifest dense periodic-like traces, also called strange attractors [3]. The trace of a continuous chaotic system can hardly pass the same point twice, but that of a discrete chaotic map can possibly pass the same point after a sufficient number of marching steps [4].

Chaotic dynamic systems emerge in many theoretical problems. In [5], a logistic map was developed to describe the evolution of population. In [6], a Lorenz system was derived to describe the coupling of Navier-Stokes equations with thermal convection, under an Oberbeck-Boussinesq approximation. In [7], a 2D chaotic map was introduced to capture the stretching and folding dynamics of a Lorenz system. In [8], a predator-prey chaotic map was used to model the population evolution of prey and predator, respectively.

Conventional chaotic dynamic systems may have limited range of system parameters [9] and low complexity [4], restricting their available key space for encryption applications. Many researches have been conducted to increase the number and range of system parameters as well as the complexity of chaotic maps [2], [4], [10], [11], [12], [13]. In [14] and [15], new chaotic dynamic systems were synthesized by combining different functions or their Taylor's series. In this work, we extend the Taylor's series of some first-order difference equations to propose a more general form of power series.

Chaotic systems have been used to enhance data security in image transmission, cryptography [16], [17] and secure communications. The complexity of a chaotic system can be

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Sharif.

evaluated with various indices, including Lyapunov exponent (LE) [10], [11], [15], correlation dimension (CD) [10], [11], growth rate K out of 0-1 test [15], [18], spectral entropy (SE) [19], and permutation entropy (PE) [20], [21].

For an N-dimensional chaotic map, N LEs can be estimated. A positive LE implies the system is chaotic, and the system is considered hyperchaotic if the number of positive LE, N_p, is two or higher. A Kaplan-Yorke dimension (D_{KY}) derived from LEs can be used to predict the dimension of the strange attractor [1]. The CD measures the dimension of the strange attractor in the N-dimensional phase space of state variables.

The growth rate K of sequence $x_n[\ell]$ measures the mean-square displacement of a 2D-trajectory in the pq plane, with $p[\ell+1] = p[\ell] + x_n[\ell]\cos(c_a\ell)$ and $q[\ell+1] = q[\ell] + x_n[\ell]\sin(c_a\ell)$. If K is close to 1, the trajectory manifests chaotic behavior like Brownian motion and the mean-square displacement increases linearly with sequence index ℓ.

The complexity of sequence $x_n[\ell]$ can be measured by examining its frequency spectrum or SE. The frequency spectrum appears more uniform if $x_n[\ell]$ is more chaotic. The PE of sequence $x_n[\ell]$ measures its complexity from possible order patterns within a given window d, and $d = 5$ was recommended in [22]. The occurrence rate of each order pattern is derived by scanning through $x_n[\ell]$, with $\ell = 1 \cdots L$.

In [4], a 2D-SCMCI hyperchaotic map was proposed by using cascade modulation couple and two 1D chaotic maps. In [23], a 2D chaotic map comprised of mod functions was optimized to yield high complexity. In [14], a chaotic map consisted of a few nonlinear terms was derived from a Cournot Duopoly game. The chaotic maps in [4], [14], and [23] were designed to achieve higher complexity, larger number and range of system parameters.

Table 1 summarizes the complexity indices of some 2D chaotic maps in the literature. These chaotic maps usually have 2-6 system parameters (SPs) and two initial conditions (ICs), yielding a key space of $2^{200\sim400}$. Typically, they have one positive LE, CD < 2, $D_{KY} < 2$, $K \leq 0.8$, SE ≤ 0.5 and PE ≤ 0.7. A force convergence (FC) mechanism is designed to ensure the convergence of two sequences a chaotic map generates. The chaotic maps with FC mechanism usually yield better performance indices of K, SE and PE than their counterparts without such mechanism.

The first chaos cryptography proposed in [31] was achieved by permutation and diffusion of pixels. A color plaintext image of size L_rL_c is stored in $3L_rL_c$ bytes of memory. Two chaotic sequences of length $L = 3L_rL_c$ were generated with a 2D chaotic system. The pixel positions of the plaintext image were permuted with the first sequence, then the permuted pixels were taken XOR with the second sequence to derive a ciphertext, which resembled $3L_rL_c$ random numbers in [0, 255] [15], [32].

In [33], an anti-dynamic degradation theorem was presented to ensure the general secrecy of chaotic cryptography systems. Consider a 1D chaotic map with system parameters in 64 bits, the generated chaotic sequences are in principle periodic due to the finite precision of system parameters. In practice, however, the period will be long enough that the probability of yielding repeated sequences is negligible. Such probability can be further reduced if higher-order chaotic maps are used [34], [35], [36].

TABLE 1. Performance indices of chaotic maps in the literature, SP: number of system parameters, IC: number of initial conditions, FC: force convergence.

2D map	SPs & ICs	key space	LEs	N_p	D_{KY}	CD
[7]	2+2	199.31	0.74, −2.47	1	1.37	1.26
[24]	2+2	199.31	1.20, −0.28	1	2	1.30
[25]	2+2	199.31	1.85, −4.17	1	1.93	1.26
[4]	4+2	298.97	4.99, −1.50	1	2	1.15
[14]	6+2	398.63	0.34, −1.01	1	1.17	0.95
[2]	4+2	298.97	0.66, −0.09	1	2	1.71
[26]	2+2	199.32	0.35, −0.21	1	2	1.84
[13]	2+2	199.32	0.35, 0.03	2	2	1.62
[11]-1	2+2	199.32	4.00, −1.67	1	2	1.87
[11]-2	2+2	199.32	2.68, 2.22	2	2	1.9
[11]-3	2+2	199.32	1.16, 1.16	2	2	2.05
[27]	4+2	298.97	0.06, −0.92	1	1.03	1.39
[28]	2+2	199.32	1.19, −1.70	1	1.59	1.51
[29]	2+2	199.32	4.45, 1.78	2	2	1.65
[30]	2+3	249.14	5.79, 5.94	2	2	2.00

2D map	K	SE	PE	FC
[7]	0.995, 0.995	0.906, 0.906	0.618, 0.619	No
[24]	0.862, 0.890	0.41, 0.550	0.554, 0.671	No
[25]	0.998, 0.998	0.698, 0.698	0.829, 0.829	No
[4]	0.998, 0.997	0.937, 0.934	0.974, 0.981	Yes
[14]	0.776, 0.341	0.850, 0.686	0.634, 0.578	No
[2]	0.728, 0.901	0.2029, 0.314	0.598, 0.592	No
[26]	0.728, 0.901	0.203, 0.314	0.598, 0.592	No
[13]	0.437, 0.839	0.147, 0.165	0.690, 0.777	No
[11] - 1	0.946, 0.958	0.944, 0.947	0.996, 0.996	Yes
[11] - 2	0.884, 0.968	0.936, 0.949	0.960, 0.996	Yes
[11] - 3	0.972, 0.972	0.947, 0.947	0.996, 0.996	Yes
[27]	0.426, 0.789	0.787, 0.851	0.589, 0.569	No
[28]	0.948, 0.948	0.948, 0.948	0.858, 0.858	Yes
[29]	0.997, 0.998	0.931, 0.944	0.972, 0.992	Yes
[30]	0.970, 0.967	0.948, 0.948	0.996, 0.996	Yes

Numerous chaotic cryptography schemes have been proposed to improve the security and efficiency of encryption. In [4], a 2D-SCMCI hyperchaotic map was used to improve the security of cryptography schemes. In [14], bit-level operations were taken to improve the security of algorithms. In [37], an image encryption scheme was proposed to achieve high encryption efficiency, based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion. In [38], an image encryption algorithm based on plane-level image filtering and discrete logarithmic transformation was proposed to balance security and efficiency. In [39], memristive chaotic systems with complex dynamics were proposed to improve the security of encryption schemes. In [17], a one-dimensional sine chaotic system (1DSCS) with large parameter interval was introduced to improve the security. In [40], an image encryption algorithm based on a roulette jump selection chaotic system and an alienated image library transformation was proposed to enhance the security.

TABLE 2. Performance indices of various image encryption methods.

crypto-graphy	encryption time (s)	$CR_h \times 10^4$	$CR_v \times 10^4$	$CR_d \times 10^4$
[45]	0.33	$80 \sim -40$	$60 \sim -60$	$80 \sim -40$
[46]	0.29	$33 \sim -29$	$20 \sim -26$	$24 \sim -24$
[14]	>1.89	-16	4	14
[17]	1.718	$75 \sim -57$	$27 \sim -39$	$67 \sim -65$
[23]	0.29	$0.79 \sim -0.64$	$0.12 \sim -4.3$	$-1.1 \sim -6.2$
[47]	> 0.26	8.27	-7.7	-4.5
[15]	0.26	$13 \sim -9$	$6 \sim -8$	$14 \sim -9$
[4]	-	$15 \sim -25$	$25 \sim -38$	$11 \sim -11$
[44]	0.50	$-16 \sim -42$	$49 \sim -7.9$	$18.5 \sim -23.3$
[38]	0.16	$19 \sim -5$	$18 \sim -25$	$22 \sim -51$
this work	0.0478	$40 \sim -24$	$46 \sim -24$	$34 \sim -18$

crypto-graphy	IE	NPCR (%)	UACI (%)
[45]	$7.9998 \sim 7.9969$	$99.626 \sim 99.587$	$33.5037 \sim 33.3954$
[46]	$7.9998 \sim 7.9998$	99.6145∼99.6009	-
[14]	$7.9976 \sim 7.9968$	99.6368∼99.5834	$33.4185 \sim 33.5832$
[17]	$7.9993 \sim 7.9992$	99.6243∼99.5945	$33.5378 \sim 33.4154$
[23]	$7.9995 \sim 7.9994$	99.6103∼99.6082	$33.4654 \sim 33.4583$
[47]	7.9976	-	-
[15]	7.99986∼7.99983	$99.614 \sim 99.6101$	$33.4965 \sim 33.4588$
[4]	$7.9973 \sim 7.9968$	$99.65 \sim 99.54$	$33.68 \sim 33.27$
[44]	$7.9993 \sim 7.9995$	$99.63 \sim 99.59$	$33.51 \sim 33.41$
[38]	$7.9992 \sim 7.9998$	$99.619 \sim 99.585$	$33.5077 \sim 33.4323$
this work	7.9998	99.61	$33.48 \sim 33.46$

Typical image encryption schemes were proposed to defend against plaintext attack and differential attack [41], [42], [43]. Their efficacy was usually evaluated in terms of key space [4], [14], key sensitivity [4], [14], [38], information entropy (IE) [13], and correlation coefficients CR_h, CR_v and CR_d in horizontal, vertical and diagonal directions, respectively [13]. A typical plaintext image has nonuniform distribution of pixel values and high correlation between adjacent pixels. The ciphertext image is preferred to have random values on pixels, implying the IE is close to 8 and the CRs are close to 0.

The resilience of an encryption scheme against exhaustion attack and occlusion attack can be evaluated with the size of key space and a structural similarity index measure (SSIM), respectively [23]. An encryption scheme with large key space is more capable of defending exhaustion attacks which try on every combination of possible keys. Occlusion attack intends to block part of the ciphertext image, which takes little effect on the decrypted image in the face of a permuted sequence.

The resilience to differential attacks can be evaluated in terms of the number of pixel change rate (NPCR) [13], unified average changing intensity (UACI) [13] and key sensitivity [4]. The NPCR gives the proportion of affected pixels in the ciphertext if one bit of the plaintext is changed. An effective image encryption scheme yields NPCR $\simeq$ 99.61%, considering the probability for two random bytes to be the same is $1/256 \simeq 0.39\%$. The UACI measures the change of pixel values. The expectation value of the absolute difference between two bytes picked from a uniform distribution in [0, 255] is 85.33, which is normalized by 255 to have UACI = 33.46%. The key sensitivity can be evaluated in terms of the NPCR and UACI of the decrypted images with exact key and perturbed key, respectively. With an effective image encryption scheme, the plaintext image cannot be recovered if the key is slightly perturbed.

Table 2 lists the performance indices of various image encryption methods. The values of IE and CRs are close to 8 and zero, respectively, confirming the randomness of ciphertext image. The NPCR and UACI are close to the ideal values of 99.61 % and 33.33 %, respectively. The slight differences among different schemes are possibly attributed to the difference of image size. The image encryption time on an image of size 512×512 is about 0.2 s with most methods.

In this work, we propose the second-order chaotic maps with optimized random coefficients to generate chaotic sequences for image encryption. Two screening conditions are proposed to identify 300 candidate chaotic maps in terms of complexity indices K and SE. A particle swarm optimization method is then applied to search for the optimal chaotic maps under eight different weighting schemes. The optimal chaotic maps are evaluated in terms of the complexity indices N_p, D_{KY}, CD, K, SE and PE. The sensitivity of all the system parameters and initial values is simulated to evaluate the security performance of the optimal chaotic maps. A hybrid sequence generation (HSG) scheme is also proposed to further reduce the image encryption time.

The rest of this work is organized as follows. The optimization of chaotic maps is presented in Section II, image encryption is presented in Section III, and some conclusions are drawn in Section IV.

II. OPTIMIZATION OF CHAOTIC MAPS

A general chaotic map can be implemented as

$$\bar{x}[\ell+1] = \bar{f}(\bar{x}[\ell])$$

where $\bar{x}[\ell] = (x_1[\ell], x_2[\ell], \cdots, x_N[\ell])$ in an N-dimensional phase space constitutes N sequences, $x_n[\ell]$, with $1 \le n \le N$. Let's consider an Mth-order power-series form of $f_n(\bar{x}[\ell])$ as

$$x_n[\ell+1] = \sum_{m_1+m_2+\cdots+m_n=m}^{m=0,1,\cdots M} a_{nm_1m_2\cdots m_n} \times x_1^{m_1}[\ell]x_2^{m_2}[\ell]\cdots x_n^{m_n}[\ell] \quad (1)$$

where m_n is the exponent of x_n and $\{a_{nm_1m_2\cdots m_n}\}$ are the system parameters.

In this work, we will focus on 2D chaotic maps (with $N = 2$), which generate two chaotic sequences to implement permutation and diffusion, respectively, on pixels for the purpose of image encryption. To provide sufficient complexity, $M = 2$ is chosen and (1) is thus reduced to

$$x_n[\ell+1] = \sum_{m_1+m_2=m}^{m=0,1,2} a_{nm_1m_2}x_1^{m_1}[\ell]x_2^{m_2}[\ell], \quad n = 1, 2 \quad (2)$$

Explicitly,

$$x_1[\ell+1] = a_{100} + a_{110}x_1[\ell] + a_{101}x_2[\ell] + a_{120}x_1^2[\ell] + a_{111}x_1[\ell]x_2[\ell] + a_{102}x_2^2[\ell] \quad (3)$$

$$x_2[\ell+1] = a_{200} + a_{210}x_1[\ell] + a_{201}x_2[\ell] + a_{220}x_1^2[\ell] + a_{211}x_1[\ell]x_2[\ell] + a_{202}x_2^2[\ell] \quad (4)$$

which take 16 multiplications to march on ℓ. To reduce the number of multiplications, (3) and (4) are rearranged as

$$x_1[\ell+1] = a_{100} + (a_{110} + a_{111}x_2[\ell] + a_{120}x_1[\ell])x_1[\ell] + (a_{101} + a_{102}x_2[\ell])x_2[\ell] \quad (5)$$

$$x_2[\ell+1] = a_{200} + (a_{210} + a_{211}x_2[\ell] + a_{220}x_1[\ell])x_1[\ell] + (a_{201} + a_{202}x_2[\ell])x_2[\ell] \quad (6)$$

which take 10 multiplications.

A. SCREENING OF INITIAL POPULATION

A chaotic map candidate is created by selecting the system parameters $a_{nm_1m_2}$'s as random numbers from a uniform distribution in $[-1, 1]$ and setting $x_1[1] = 0.5$ and $x_2[1] = 0.5$. Then, (5) and (6) are used to generate sequences $x_1[\ell]$'s and $x_2[\ell]$'s of length $L_t = L + L_{ig} = 10,500$, where $L = 10,000$ is the preplanned length and $L_{ig} = 500$ is the extended length. If the two sequences do not diverge, the first L_{ig} elements of each sequence are removed to form two new sequences $x_1[\ell]$'s and $x_2[\ell]$'s of length L.

By trial and error, we get 22 viable chaotic maps accompanied with 184 divergent maps. If the range of system parameters is extended to $[-1.5, 1.5]$, we get 9 viable chaotic maps accompanied with 253 divergent maps. Similarly, if the range is extended to $[-2, 2]$, we get 5 viable chaotic maps accompanied with 274 divergent maps. It seems adopting a wider range reduces the number of viable chaotic maps although the key space for encryption is increased. As a trade-off, the range of $[-1, 1]$ is adopted in this work.

Based on the literature survey listed in Table 1, we set a condition for screening the initial population of chaotic map candidates as

$$(\max K > 0.5) \text{ or } (\max \text{SE} > 0.5) \quad (7)$$

where high growth rate K tends to exclude stand-still sequences [23] and high SE favors sequences with spectral power resembling white noise. This condition admits candidates with at least one of the complexity indices, K_1, K_2, SE_1 and SE_2, greater than 0.5.

Fig.1 shows the complexity indices of 300 maps that satisfy the screening condition (7), which are relabeled in an ascending order of their K_1 index. The indices K, SE and PE of sequence $x_n[\ell]$ is labeled as K_n, SE_n, and PE_n, respectively, with $n = 1, 2$.

Fig.1(a) shows that more than 50% of the maps have $K_1 = 0.12$ or $K_2 = 0.12$. We arbitrarily set a threshold of $K_1 = 0.8$, marked by the dashed line, to distinguish between chaotic maps and non-chaotic ones. Figs.1(b)- 1(f) confirm that this dashed line also roughly separates chaotic maps from

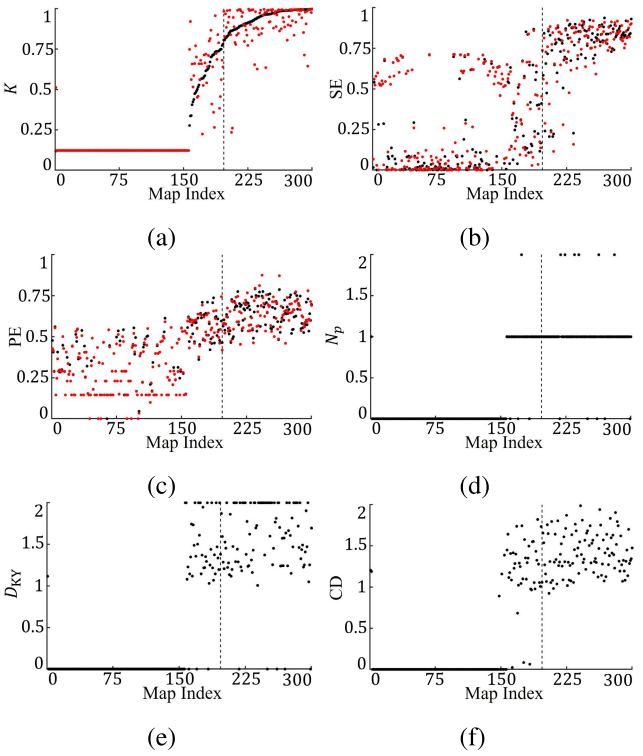

FIGURE 1. Complexity indices of 300 chaotic maps satisfying (7), relabeled in ascending order of K_1 index, (a) •: K_1, •: K_2, (b) •: SE_1, •: SE_2, (c) •: PE_1, •: PE_2, (d) N_p, (e) D_{KY}, (f) CD.

non-chaotic ones in terms of the other five chaotic indices. Fig.1(b) shows that the maps before map index 197 have $\max\{\text{SE}\} < 0.75$, although some maps with low SE exist between map indices 197 to 259. Fig.1(c) shows that the maps after map index 197 have PE > 0.4. Figs.1(d)-1(f) show that most of the maps after map index 197 have $N_p \geq 1$, $D_{KY} > 1$ and CD> 0.9.

Based on these observations, a more strict screening condition is set as

$$(\min K > 0.8) \text{ and } (\min \text{SE} > 0.8) \quad (8)$$

Fig.2 shows the complexity indices of 300 maps that satisfy (8), which are relabeled in ascending order of K_1 index. These maps in general have PE > 0.5, $N_p \geq 1$, $D_{KY} > 1$ and CD > 1, in addition to $K > 0.8$ and SE > 0.8 as set in (8). Fig.2(b) shows that the SE falls within $[0.8, 0.95]$. Fig.2(c) shows that most maps have PE falling within $[0.5, 0.8]$. By comparing Fig.2 and Fig.1, (8) is proven a more effective condition for screening chaotic maps.

Figs.3(a) and 3(b) show the distribution of 12 system parameters in 300 chaotic maps generated under the screening conditions of (7) and (8), respectively. Each system parameter of the 300 chaotic maps roughly follows a uniform distribution in $[-1, 1]$, under either screening condition.

In conventional chaos encryption, the system parameters of a chaotic map are used as keys, and the key space is determined by the range of system parameters. Encryptions with

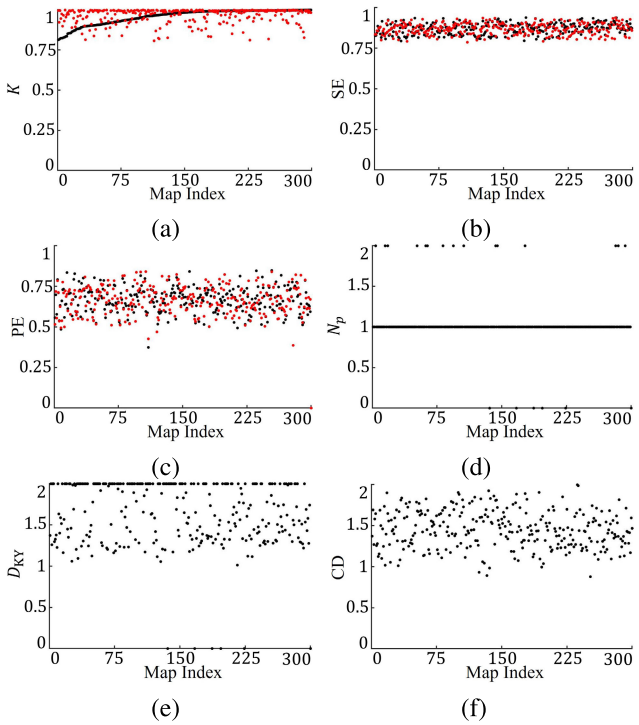

FIGURE 2. Complexity indices of 300 chaotic maps satisfying (8), relabeled in ascending order of K_1 index, (a) •: K_1, •: K_2, (b) •: SE_1, •: SE_2, (c) •: PE_1, •: PE_2, (d) N_p, (e) D_{KY}, (f) CD.

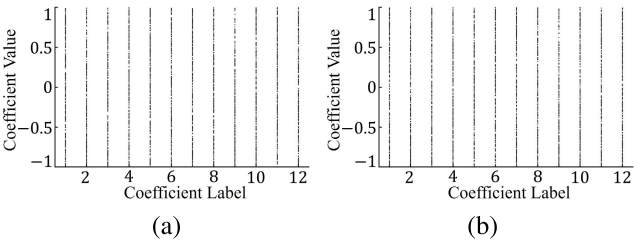

FIGURE 3. Distribution of coefficients in 300 chaotic maps, (a) under condition (7), (b) under condition (8).

larger key space are more resilient to attacks. In most chaotic maps, the range of system parameters are restricted to a small range or have discontinuity within the preplanned range. A viable chaotic map remains chaotic if the system parameters are slightly perturbed.

B. PHASE PORTRAITS OF CHAOTIC MAPS

Fig.4 shows the phase portrait of four chaotic maps picked from the 300 chaotic maps screened with (7). Their system parameters are listed in Table 3. Fig.4(a) manifests three clusters of points and and Fig.4(b) manifests six clusters of points.

Fig.5(a) shows the phase portrait of M-w$_1$ for closer inspection, with points in the three clusters marked by different colors. Figs.5(b) and 5(c) illustrate that the elements of $x_1[\ell]$ or $x_2[\ell]$ jump alternately from one cluster to another, as tracked by color.

TABLE 3. System parameters (SP) of chaotic maps M-w$_{1,2,3,4}$ and M-s$_{1,2,3,4}$.

label	SP	M-w$_1$	M-w$_2$	M-w$_3$	M-w$_4$
1	a_{100}	0.175	0.6204	0.945	−0.270
2	a_{110}	−0.806	0.450	−0.045	−0.951
3	a_{101}	0.548	−0.629	−0.999	0.754
4	a_{120}	−0.347	−0.091	−0.123	0.717
5	a_{111}	0.068	0.167	−0.379	0.033
6	a_{102}	−0.143	−0.781	−0.975	0.790
7	a_{200}	0.899	0.143	−0.583	−0.408
8	a_{210}	−0.642	0.341	0.076	−0.985
9	a_{201}	−0.544	0.503	−0.537	−0.301
10	a_{220}	−0.588	0.914	−0.647	−0.622
11	a_{211}	−0.664	0.376	0.614	0.401
12	a_{202}	−0.749	−0.245	0.134	0.419
label	SP	M-s$_1$	M-s$_2$	M-s$_3$	M-s$_4$
1	a_{100}	−0.668	0.861	−0.465	−0.756
2	a_{110}	−0.537	−0.667	−0.913	0.127
3	a_{101}	−0.896	0.579	−0.586	0.776
4	a_{120}	0.804	−0.794	−0.029	0.720
5	a_{111}	0.587	0.767	0.524	−0.623
6	a_{102}	−0.254	0.045	−0.358	0.383
7	a_{200}	0.664	0.948	−0.412	−0.712
8	a_{210}	0.508	0.512	0.893	0.161
9	a_{201}	0.244	0.445	−0.926	0.007
10	a_{220}	−0.212	−0.995	0.9006	−0.779
11	a_{211}	−0.281	−0.589	−0.368	−0.051
12	a_{202}	−0.822	−0.479	0.983	0.291

TABLE 4. Complexity indices of chaotic maps M-w$_{1,2,3,4}$ and M-s$_{1,2,3,4}$.

model	LE	N_p	D_{KY}	CD
M-w$_1$	0.381, −0.403	1	1.95	1.58
M-w$_2$	0.144, −0.111	1	2	1.73
M-w$_3$	0.194, 0.0007	2	2	1.74
M-w$_4$	0.3480, −0.5592	1	1.62	1.07
M-s$_1$	0.2017, −0.6727	1	1.30	1.35
M-s$_2$	0.4201, −0.1005	1	2	1.69
M-s$_3$	0.4151, 0.0588	2	2	1.7821
M-s$_4$	0.3584, −0.7482	1	1.48	1.30
[2]	0.6586, −0.0918	1	2	1.7097
[14]	0.7367, −0.9845	1	1.7482	0.9473
[4]	4.9992, −1.5023	1	2	1.1498

model	K	SE	PE
M-w$_1$	0.6205, 0.5412	0.1399, 0.1255	0.4778, 0.4760
M-w$_2$	0.7811, 0.6397	0.4100, 0.4544	0.5958, 0.7442
M-w$_3$	0.5801, 0.7144	0.6730, 0.6691	0.7100, 0.6929
M-w$_4$	0.9222, 0.8026	0.6744, 0.6152	0.6213, 0.5728
M-s$_1$	0.9956, 0.9337	0.8765, 0.8072	0.7429, 0.7529
M-s$_2$	0.8340, 0.9544	0.8484, 0.8553	0.7297, 0.7763
M-s$_3$	0.9469, 0.9977	0.8730, 0.9025	0.6985, 0.7894
M-s$_4$	0.9902, 0.9546	0.8521, 0.8659	0.6662, 0.6803
[2]	0.7277, 0.9007	0.2029, 0.3141	0.5979, 0.5921
[14]	0.7759, 0.3412	0.8502, 0.6862	0.6342, 0.5784
[4]	0.9982, 0.9965	0.9370, 0.9341	0.9744, 0.9807

Fig.6 shows a similar phase portrait with two clusters [2]. The elements of either sequence jump alternately between these two clusters.

Clustering in phase portrait and alternating sequences are correlated to low SEs and low PEs, as listed in Table 4. For example, M-w$_1$ has SEs of 0.1399, 0.1255 and PEs of

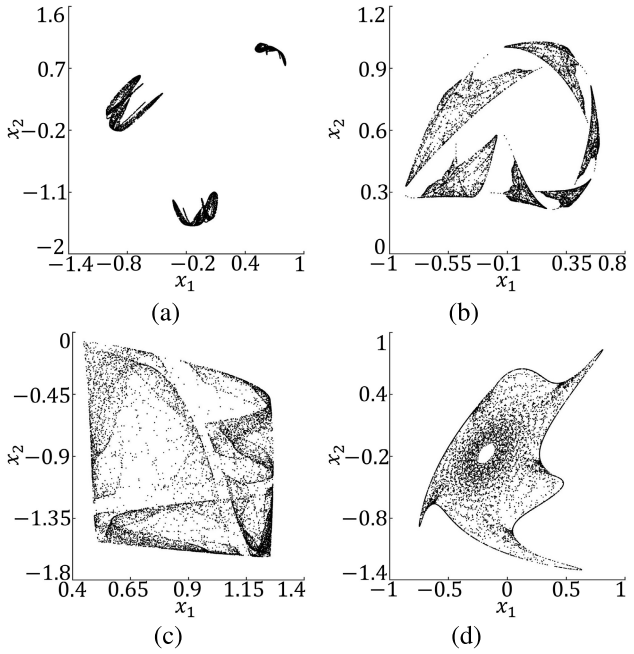

FIGURE 4. Phase portraits of chaotic maps among 300 chaotic maps screened with (7), $L = 10,000$, (a) M-w$_1$ with $N_P = 1$, $D_{KY} = 1.95$ and CD = 1.58, (b) M-w$_2$ with $N_P = 1$, $D_{KY} = 2$ and CD = 1.73, (c) M-w$_3$ with $N_P = 2$, $D_{KY} = 2$ and CD = 1.74, (d) M-w$_4$ with $N_P = 1$, $D_{KY} = 1.62$ and CD = 1.07.

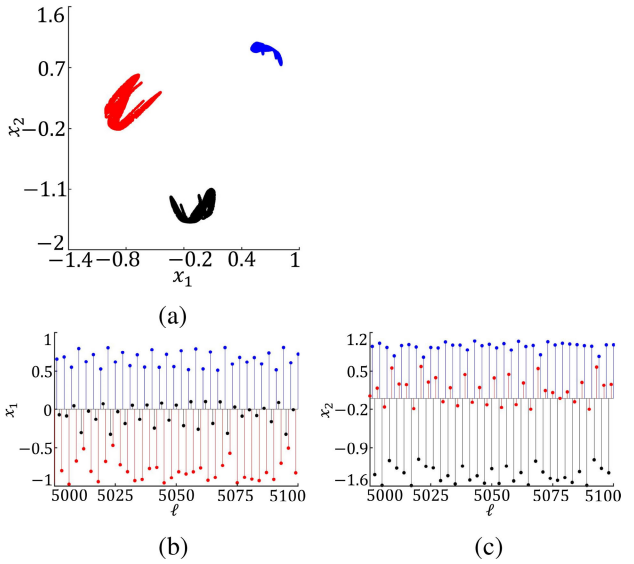

FIGURE 5. (a) Phase portrait of M-w$_1$, (b) $x_1[\ell]$, (c) $x_2[\ell]$.

0.4778, 0.4760; M-w$_2$ has SEs of 0.1399, 0.1255 and PEs of 0.5958, 0.7442.

M-w$_1$ has lower PEs than M-w$_2$, attributed to gaps in sequences of M-w$_1$. For M-w$_1$, no elements of $x_1[\ell]$ fall in [0.1, 0.4] and no elements of $x_2[\ell]$ fall in $[-1.1, -0.3]$. For M-w$_2$, $x_1[\ell]$'s fall in $[-0.6, 0.57]$ and $x_2[\ell]$'s fall in [0.3, 1], without gap or discontinuity.

The complexity indices N_p, D_{KY} and CD characterize the dimension of the strange attractor. The Lyapunov exponents (LEs) in an N-dimensional phase space measure N separation

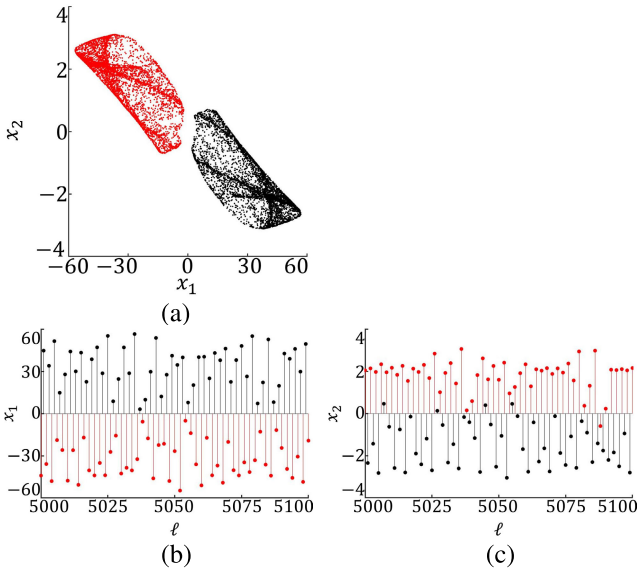

FIGURE 6. (a) Phase portraits of 2D chaotic maps [2], with $L = 10^4$, $N_p = 1$, $D_{KY} = 2$, CD = 1.71. (b) $x_1[\ell]$, (c) $x_2[\ell]$.

rates, of sequences generated with a given chaotic map, in N independent directions from a starting point [48], which are used to evaluate the complexity of the chaotic map [15], [20], [49], [50]. The number N_p of positive LEs indicates the dimension of the strange attractor. However, LEs may fluctuate around zeros, yielding ambiguous N_p. Take Fig.4(d) of map M-w$_4$ for example, despite the 2D-like strange attractor, its N_p value is one.

The D_{KY} derived with Kaplan-Yorke formula estimates the dimension of the strange attractor [51]. Higher D_{KY} implies larger N_p hence higher complexity. Take chaotic map M-w$_1$ for example, it has LEs of 0.381 and -0.403, yielding $D_{KY} = 1 + 0.381/0.103 = 1.95$. It seems D_{KY} tends to overestimate the dimension of the strange attractor.

The correlation dimension (CD) measures the dimension of the distribution formed by the N-sequences in the phase space. An N-dimensional map with CD close to N has high complexity. The dimension of the strange attractor can be estimated more accurately with the CD index, but its computational time is $O(L^2)$, as compared to $O(L)$ for computing the other indices.

As listed in Table 4, chaotic maps with high-dimensional strange attractor is expected to have better encryption performance. For a chaotic map with 1D-like phase portraits, the value of x_1 can be used to predict x_2.

Figs.4(a) and 4(b) manifest clusters in the phase portraits, forming partial 2D stranger attractors. Hence, M-w$_1$ has $N_p = 1$, $D_{KY} = 1.95$, CD = 1.58, and M-w$_2$ has $N_p = 1$, $D_{KY} = 2$, CD = 1.73. The phase portrait in Fig.4(c) appears continuous over 2D region. Chaotic maps with 2D-like strange attractor typically have $N_p = 1$, high D_{KY} and high CD, as exemplified in Table 4 that M-w$_3$ has $N_p = 2$, $D_{KY} = 2$ and CD = 1.74. Fig.4(d) manifests a 2D-like

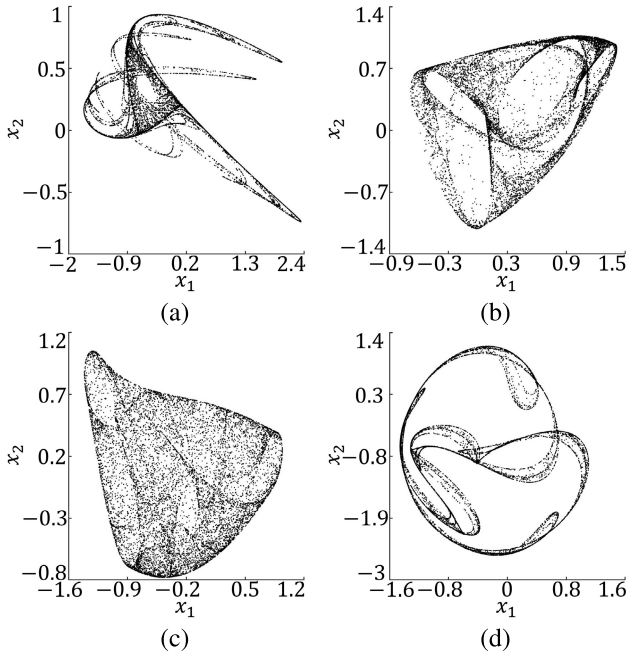

FIGURE 7. Phase portraits of chaotic maps among 300 chaotic maps screened with (8), $L = 10,000$, (a) M-s$_1$ with $N_p = 1$, $D_{KY} = 1.30$ and CD = 1.35, (b) M-s$_2$ with $N_p = 1$, $D_{KY} = 2$ and CD = 1.69, (c) M-s$_3$ with $N_p = 2$, $D_{KY} = 2$ and CD = 1.71, (d) M-s$_4$ with $N_p = 1$, $D_{KY} = 1.48$ and CD = 1.30.

strange attractor, but with many elements falling on the contour, hence its CD index is only 1.07.

Fig.7 shows the phase portraits of four maps picked from the 300 chaotic maps generated under (8), with their system parameters listed in Table 3. Figs.7(a) and 7(b) manifest 2D-like strange attractors, which are less evenly distributed as compared with that in Fig.7(c). Hence, the CD indices of M-s$_1$ and M-s$_2$ are 1.35 and 1.69, respectively, smaller than 1.78 of M-s$_3$.

Since condition (8) implies $\mathrm{SE}_1, \mathrm{SE}_2 > 0.8$, clustering features as in Figs.4(a) and 4(b) are less likely to appear. Thus, no gaps are likely to appear in the values of $x_1[\ell]$ and $x_2[\ell]$, which is correlated to higher PE, as confirmed in Table 4.

Maps satisfying the condition in (7) are more likely to generate sequences with finite period or converging to a fixed point. Such maps are likely to be screened out under condition (8). The maps satisfying the condition in (8) are likely to have higher values of K, SE and PE indices.

Next, a particle swarm optimization (PSO) algorithm is proposed to fine-tune the system parameters of chaotic maps in terms of N_p, D_{KY}, CD, K, PE and SE.

C. OPTIMIZATION OF SYSTEM PARAMETERS WITH PSO ALGORITHM

Next, a particle swarm optimization (PSO) algorithm is developed to boost the complexity of chaotic maps to the highest possible level by optimizing the system parameters $a_{nm_1m_2}$'s. The objective function is defined in terms of the complexity indices N_p, D_{KY}, CD, K, SE and PE as

$$\begin{aligned}\xi = {} & \alpha_{N_p}\frac{1}{1+N_p} + \alpha_{D_{KY}}\frac{1}{1+D_{KY}} + \alpha_{\mathrm{CD}}\frac{1}{1+\mathrm{CD}} \\ & + \alpha_K\left(1+\sum_{n=1}^{N}K_n\right)^{-1} + \alpha_{\mathrm{SE}}\left(1+\sum_{n=1}^{N}\mathrm{SE}_n\right)^{-1} \\ & + \alpha_{\mathrm{PE}}\left(1+\sum_{n=1}^{N}\mathrm{PE}_n\right)^{-1} \end{aligned} \tag{9}$$

where α's are the weighting coefficients on different complexity indices. The ranges of these indices are $\{N_p|N_p = 0, 1, 2\}$, $\{D_{KY}|0 \le D_{KY} \le 2\}$, $\{\mathrm{CD}|\mathrm{CD} \ge 0\}$, $\{K_n|0 \le K_n \le 1\}$, $\{\mathrm{SE}_n|0 < \mathrm{SE}_n < 1\}$ and $\{\mathrm{PE}_n|0 < \mathrm{PE}_n < 1\}$. The denominator of each term is added by one to avoid possible numerical singularity.

The 300 chaotic maps screened with condition (7) or (8) are used as the initial particles of the PSO algorithm. The system parameters $a_{nm_1m_2}$'s of the pth chaotic map are equivalent to the position coordinates of the pth particle, $\bar{r}_p^{(g)}$, where the superscript g means the gth iteration. The position $\bar{r}_p^{(g)}$ and velocity $\bar{v}_p^{(g)}$ of the pth particle are updated as

$$\begin{aligned}\bar{v}_p^{(g+1)} &= v_\mu\bar{v}_p^{(g)} + p_\mu\bar{w}_p(\bar{r}_{pb}^{(g)} - \bar{r}_p^{(g)}) + g_\mu\bar{w}_g(\bar{r}_{gb}^{(g)} - \bar{r}_p^{(g)}) \\ \bar{r}_p^{(g+1)} &= \bar{r}_p^{(g)} + \bar{v}_p^{(g+1)}\end{aligned}$$

where v_μ is the inertial weight, p_μ is the personal weight, g_μ is the social weight, $\bar{r}_{gb}$ is the global best position, $\bar{r}_{pb}$ is the personal best position of particle p, $\bar{w}_p = \{w_{p1}, w_{p2}, \cdots, w_{pN}\}$ and $\bar{w}_g = \{w_{g1}, w_{g2}, \cdots, w_{gN}\}$ are weighting vectors, with w_{pn} and w_{gn} random numbers uniformly distributed in [0, 1]. In this work, we choose $v_\mu = 0.8$, $p_\mu = 0.1$ and $g_\mu = 0.1$.

D. OPTIMAL CHAOTIC MAPS UNDER DIFFERENT WEIGHTING SCHEMES

Table 5 lists the complexity indices of the optimal chaotic maps under different weighting schemes, which are labeled as uni-s/w, K-s/w, SE-s/w, PE-s/w, respectively, pending on the weighting vector $\bar{\alpha} = [\alpha_{N_p}, \alpha_{D_{KY}}, \alpha_{\mathrm{CD}}, \alpha_K, \alpha_{\mathrm{SE}}, \alpha_{\mathrm{PE}}]$. The uni scheme is assigned with uniform weighting coefficients of $\alpha = 1$, the K scheme, SE scheme and PE scheme are assigned with $\alpha_K = 100$, $\alpha_{SE} = 100$ and $\alpha_{PE} = 100$, respectively, while the other α coefficients are set to one. The attached labels w and s indicate the weak condition in (7) and the strong condition in (8), respectively.

Performance indices N_p and D_{KY} are not assigned with large weighting coefficients because the maximum values of $N_p = 2$ and $D_{KY} = 2$ are relatively easy to achieve. The value of LE varies slightly as L is incremented, leading to alternation of N_p between 1 and 2.

The CD index characterizes the dimension of a strange attractor, but it cannot distinguish between chaotic and non-chaotic maps. For example, a stationary 2-sequence with $x_1[\ell] = 0$ and $x_2[\ell] = 0$ for all ℓ has an infinite CD index.

From the simulation results, we observe that under the K-s/w scheme, the resulting sequences manifest Brownian-like motion in the pq plane. Under the SE-s/w scheme, the

resulting sequences behave like white noise in the spectral domain. Under the PE-s/w scheme, adjacent elements in the resulting sequences possess unbiased ordering pattern. Similar observations will be elaborated in the rest of this Section.

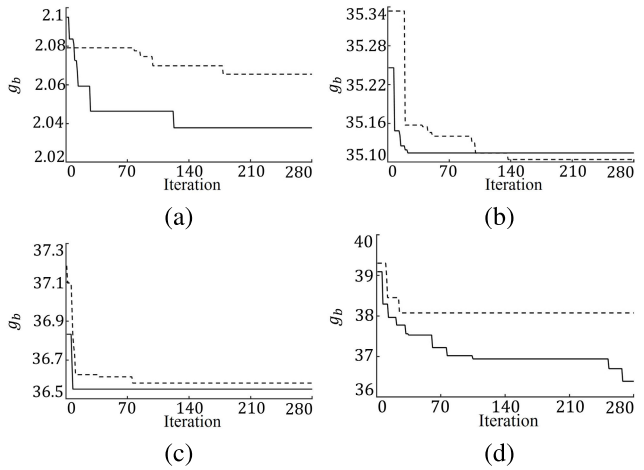

FIGURE 8. Iteration of global best objective function under weighting scheme of (a) uni-s/w, (b) K-s/w, (c) SE-s/w, (d) PE-s/w. ——: screened with (8), – – –: screened with (7).

Fig.8 shows the iteration of global best objective function g_b under weighting schemes of uni-s/w, K-s/w, SE-s/w and PE-s/w, respectively. It is observed that the objective function converges faster if the chaotic maps are screened with (8) instead of (7). The initial value of g_b screened with (8) is lower than that with (7).

Given a perfect chaotic map with the highest possible complexity indices of $N_p = 2$, $D_{KY} = 2$, CD $= 2$, $K_1 = K_2 = 1$, $\text{SE}_1 = \text{SE}_2 = 1$ and $\text{PE}_1 = \text{PE}_2 = 1$, the objective function under the weighting scheme of K, SE or PE in (9) will be 35. The distributions of K, SE and PE in Figs.1 and 2, show that SE and PE are capped by 0.95 and 0.8, respectively. Hence, the global best objective function under weighting schemes of SE-s/w and PE-s/w are more difficult to converge to the ideal value of 35 than that under weighting scheme of K-s/w.

Table 5 shows that uni-s scheme achieves complexity indices of CD $=$ 2.0387, $K = [0.9917, 0.9942]$, SE $= [0.9335, 0.9380]$ and PE $= [0.8735, 0.9131]$, which are higher than their counterparts of uni-w scheme, with CD $= 2.0292$, $K = [0.9493, 0.9631]$, SE $= [0.8868, 0.9070]$ and PE $= [0.8440, 0.8776]$. The K-s scheme achieves the highest K of 0.9990 and higher CD of 1.9138 than 1.8845 under K-w scheme. The SE-s scheme achieves higher SE $= [0.9463, 0.9461]$ than SE $= [0.9465, 0.9380]$ under SE-w scheme. The PE-s scheme achieves higher PE $= [0.9495, 0.9409]$ than PE $= [0.8742, 0.8762]$ under PE-w scheme.

Table 6 lists the system parameters of the optimal chaotic maps under different weighting schemes. It is observed that several system parameters are out of the initial range of $[-1, 1]$, for example, $a_{101} = 1.74$ under SE-w scheme and $a_{100} = 2.172$ under PE-s scheme.

TABLE 5. Complexity indices of optimal chaotic maps screened with condition (7) or (8).

model	α_{N_p}	$\alpha_{D_{KY}}$	α_{CD}	α_K	α_{SE}	α_{PE}
uni	1	1	1	1	1	1
K	1	1	1	100	1	1
SE	1	1	1	1	100	1
PE	1	1	1	1	1	100

model	LE	N_p	D_{KY}	CD
uni-w	0.5414, 0.2039	2	2	2.0292
K-w	0.4748, 0.0303	2	2	1.8845
SE-w	0.8807, −0.5873	1	2	1.8875
PE-w	0.5130, 0.1596	2	2	1.8783
uni-s	0.6790, 0.1224	2	2	2.0387
K-s	0.5269, 0.0799	2	2	1.9138
SE-s	0.9600, −0.8442	1	2	1.5262
PE-s	0.9076, 0.6096	2	2	1.8273
[14]	0.7367, −0.9845	1	1.7482	0.9473
[4]	4.9992, −1.5023	1	2	1.1498
[2]	0.6586, −0.0918	1	2	1.7097
[13]	0.3525, 0.0272	2	2	1.6239

model	K	SE	PE
uni-w	0.9493, 0.9631	0.8868, 0.9070	0.8440, 0.8776
K-w	0.9978, 0.9986	0.9281, 0.9221	0.8795, 0.8515
SE-w	0.9829, 0.9955	0.9465, 0.9380	0.7844, 0.7231
PE-w	0.9097, 0.9781	0.8813, 0.9098	0.8742, 0.8762
uni-s	0.9917, 0.9942	0.9335, 0.9380	0.8735, 0.9131
K-s	0.9970, 0.9990	0.9379, 0.9172	0.8197, 0.8338
SE-s	0.9884, 0.9951	0.9463, 0.9461	0.7294, 0.6901
PE-s	0.9964, 0.9982	0.9404, 0.9465	0.9495, 0.9409
[14]	0.7759, 0.3412	0.8502, 0.6862	0.6342, 0.5784
[4]	0.9982, 0.9965	0.9370, 0.9341	0.9744, 0.9807
[2]	0.7277, 0.9007	0.2029, 0.3141	0.5979, 0.5921
[13]	0.6164, 0.8599	0.1475, 0.2391	0.6898, 0.7766

TABLE 6. System parameters (SP) of optimal chaotic maps under different weighting schemes.

label	SP	uni-w	K-w	SE-w	PE-w
1	a_{100}	0.376	0.132	−0.154	0.208
2	a_{110}	0.837	0.890	−0.103	0.843
3	a_{101}	−0.590	1.042	1.74	−0.522
4	a_{120}	−0.057	−0.306	0.449	−0.049
5	a_{111}	−0.634	−0.671	−0.182	−0.653
6	a_{102}	−0.483	−0.218	0.780	−0.185
7	a_{200}	−0.184	−0.582	0.935	−0.285
8	a_{210}	−0.892	−1.263	0.726	−0.967
9	a_{201}	−0.253	−0.406	−0.153	−0.323
10	a_{220}	0.125	1.239	−0.349	0.189
11	a_{211}	0.105	−0.926	0.586	0.024
12	a_{202}	0.721	0.881	−1.141	0.715

label	SP	uni-s	K-s	SE-s	PE-s
1	a_{100}	−0.118	−0.629	−0.087	2.1720
2	a_{110}	−0.124	−0.042	−0.702	−0.736
3	a_{101}	0.774	−0.426	−0.204	−0.608
4	a_{120}	−0.408	0.418	0.210	−0.236
5	a_{111}	0.256	0.769	0.1964	−0.129
6	a_{102}	1.028	0.447	0.749	−0.945
7	a_{200}	0.910	−0.693	−0.828	0.6276
8	a_{210}	0.935	1.236	−0.388	−1.040
9	a_{201}	0.448	−0.948	−1.001	0.719
10	a_{220}	−0.479	−0.176	0.634	−0.346
11	a_{211}	−0.327	−0.833	0.609	0.459
12	a_{202}	−0.160	0.653	0.9601	0.076

Fig.9 shows the phase portrait of the optimal chaotic maps. Except that under SE-s scheme, all the other phase portraits manifest 2D strange attractor, correlated to CD > 1.8.

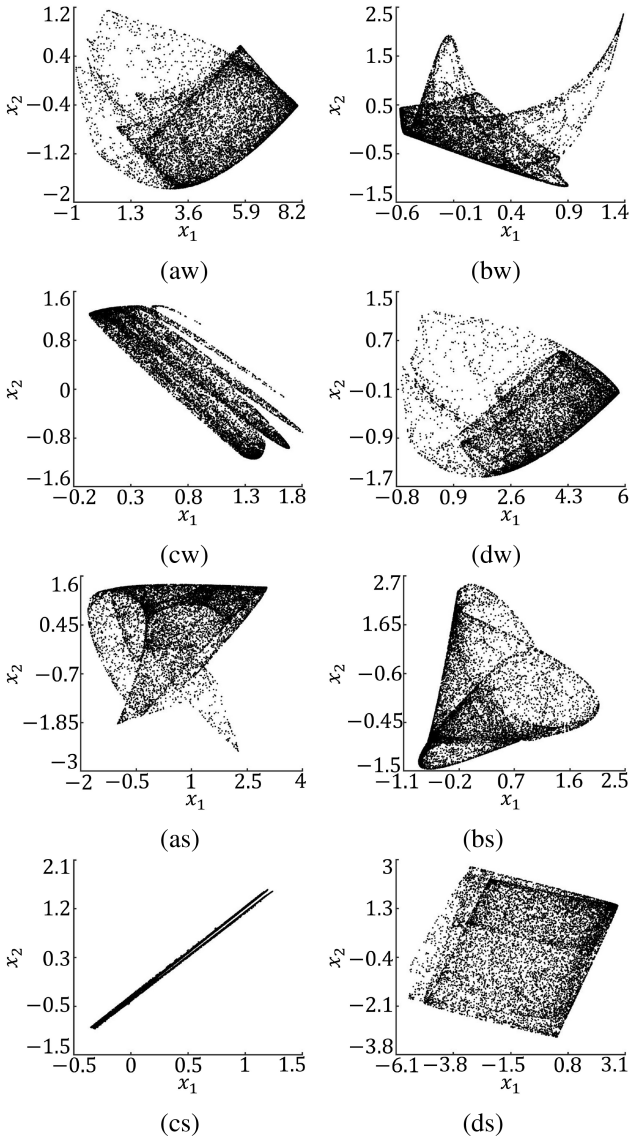

FIGURE 9. Phase portrait under scheme of (aw) uni-w, (bw) K-w, (cw) SE-w, (dw) PE-w, (as) uni-s, (bs) K-s, (cs) SE-s, (ds) PE-s, with $L = 10,000$.

The strange attractor is preferred to be 2D than 1D for the purpose of image encryption.

The phase portrait in Fig.9(dw) resembles that in Fig.9(aw), and their system parameters are also comparable.

Table 5 shows that uni-w and uni-s schemes achieve $N_p = 2$, $D_{KY} = 2$ and CD $\simeq 2$. The uni-s scheme achieves SE of [0.9335, 0.9380], higher than [0.8868, 0.9070] under uni-w scheme.

Fig.9(aw) manifests a larger low-density area than in Fig.9(as), implying the former has lower SE than in the latter. In general, larger and more uniform phase portrait imply higher SE.

Fig.9(cw) displays a 2D strange attractor composed of line features, with CD = 1.888. Fig.9(cs) displays a 1D-like strange attractor, with CD = 1.526. It seems an SE scheme tends to manifest line-like features in the phase portrait.

The phase portrait shown in Fig.9(ds) manifests square regions with slightly different density, similar to that shown in Fig.10 [4]. The PE-s achieves good complexity indices of $K = 0.9964, 0.9982$, SE $= 0.9404, 0.9465$ and PE $= 0.9495, 0.9409$.

E. DEMONSTRATION UNDER UNI-S SCHEME

Fig.11(a) shows the system parameters of top 10 chaotic maps rated by their objective functions, optimized under the uni-s weighting scheme on candidates screened with (8). The red diamonds mark the system parameters of the best chaotic map, which are also listed in Table 6. Note that some coefficients lie beyond the range of $[-1, 1]$.

Fig.11(b) shows the phase portrait of the associated 2-sequences, with length $L = 4000$. The phase portrait manifests a 2D patch with relatively uniform distribution.

Fig.11(c) shows the phase portrait of the 2-sequences with length $L = 10000$. The patches become more conspicuous compared to those in Fig.11(b). Table 5 shows that the LEs characterizing the separation rate of the 2-sequences are 0.6790 and 0.1224, leading to $N_p = 2$, $D_{KY} = 2$ and CD $= 2.0387$, consistent with a 2D-like strange attractor.

Figs.12(a) and 12(b) show the probability (power spectrum) of $x_1[\ell]$ and $x_2[\ell]$, respectively, with $L = 10000$. Figs.12(c) and 12(d) show their counterparts with $L = 4000$. The probability distributions with two different sequence lengths L appear similar. The probability distributions of $x_1[\ell]$ and $x_2[\ell]$ are relatively uniform, associated with SE $= 0.9335, 0.9380$.

Let's define the p and q sequences of a sequence $x[\ell]$ with length L as [52]

$$p[\ell] = \sum_{\ell'=1}^{\ell-1} x[\ell'-1]\cos[c_a(\ell'-1)] \tag{10}$$

$$q[\ell] = \sum_{\ell'=1}^{\ell-1} x[\ell'-1]\sin[c_a(\ell'-1)] \tag{11}$$

where $p[1] = 0$, $q[1] = 0$, and c_a is a number randomly picked from $(0, 2\pi)$, excluding π. Eqns.(10) and (11) become conventional cosine and sine transforms, respectively, if the upper bound of summation is fixed at $L-1$ and $c_a = 2\pi(\ell-1)/L$.

If a sequence $x[\ell]$ manifests regular features, a circular pq trace will emerge. Take $x[\ell] = \cos(c'_a\ell)$ for example, with $0 < c'_a - c_a \ll 1$, the pq sequences are

$$\begin{aligned} p[\ell] &= \sum_{\ell'=1}^{\ell-1} \cos[c'_a(\ell'-1)]\cos[c_a(\ell'-1)] \\ &\simeq \frac{1}{4\sin(c_{a2}/2)}\sin\frac{(2\ell-3)c_{a2}}{2} + \frac{1}{4} \end{aligned} \tag{12}$$

$$\begin{aligned} q[\ell] &= \sum_{\ell'=1}^{\ell-1} \cos[c'_a(\ell'-1)]\sin[c_a(\ell'-1)] \\ &\simeq \frac{1}{4\sin(c_{a2}/2)}\left[\cos\frac{(2\ell-3)c_{a2}}{2} + \cos\frac{c_{a2}}{2}\right] \end{aligned} \tag{13}$$

where $c_{a2} = c'_a - c_a \simeq 0$.

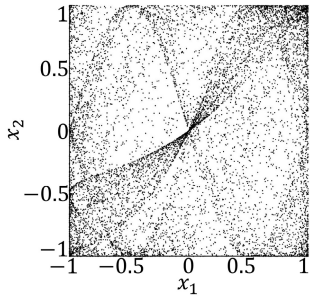

FIGURE 10. Phase portrait of chaotic map in [4], with $L = 10000$, CD = 1.15, $N_p = 1$, $D_{KY} = 2$.

In this work, 200 c_a's are randomly picked from a uniform distribution in $(0, 2\pi)$ to compute the pq sequences with (10) and (11) [52]. Then, the $p$and q sequences are used to compute a mean-square displacement $M[\ell]$, which is the sum of the power spectra at c_a of elements $x[\ell' + 1], \cdots, x[\ell' + \ell]$. For a regular sequence like $x[\ell] = \cos(c'_a \ell)$, there are two spikes at $\ell/L = c'_a$ on the power spectrum. For a chaotic sequence, $M[\ell]$ will increase with ℓ, regardless of c_a. A correlation coefficient of $M[\ell]$ and ℓ is computed for each of the 200 c_a's. These correlation coefficients are then averaged to yield the growth rate K. The growth rates of $K = 0$ and $K = 1$ indicate a regular map and a highly chaotic map, respectively [4], [18], [23].

Figs.13(a) and 13(b) show the evolution of p and q sequences, respectively, of a sequence $x[\ell] = \cos(c'_a \ell)$, with $c'_a = 0.11$ and $c_a = 0.1008$. The sequences derived with complete and approximate forms are very close. Fig.13(c) shows the corresponding pq trace of complete form and approximate form, respectively. Both traces appear to be circular. Fig.13(d) shows the pq traces of the sequence $x[\ell] = \cos(c'_a \ell)$ with $c'_a = 0.11$ and $c_a = 2\pi(c_\ell/200)$ with $c_\ell = 1, 2, \cdots, 200$. The traces are composed of multiple rings and the growth rate is $K = 0.0446$.

Figs.14(a1) and 14(a2) show the pq traces of $x_1[\ell']$ and $x_2[\ell']$, respectively, with $c_a = 2\pi(123/200)$, under uni-s scheme. Both traces appear chaotic. In contrast, Figs.14(b1) and 14(b2) show the pq traces of $x_1[\ell']$ and $x_2[\ell']$, respectively, with $c_a = 2\pi(1/200)$, under uni-s scheme. The ring-like pattern indicates a regular map.

Figs.15(a1) and 15(a2) show the pq traces of $x_1[\ell']$ and $x_2[\ell']$, respectively, under uni-s scheme, with $c_a = 2\pi(c_\ell/200)$ and $c_\ell = 1, 2, \cdots, 200$. Most pq traces are chaotic and manifest Brownian-like features. There are a few ring-like patterns immersed in the pq traces, attributed to specific c_a's as demonstrated in Figs.14(b1) and 14(b2).

Figs.15(b1) and 15(b2) show the pq traces of $x_1[\ell']$ and $x_2[\ell']$, respectively, under K-s scheme, with $c_a = 2\pi(c_\ell/200)$ and $c_\ell = 1, 2, \cdots, 200$. No regular traces as in Figs.15(a1) and 15(a2) are observed. The K indices are $K_1 = 0.9970$, $K_2 = 0.9990$, slightly higher than their counterparts of $K_1 = 0.9917$, $K_2 = 0.9942$, under uni-s scheme. Figs.15(c1) and 15(c2) show the pq traces in [4], which manifest similar features to those in Figs.15(b1) and 15(b2).

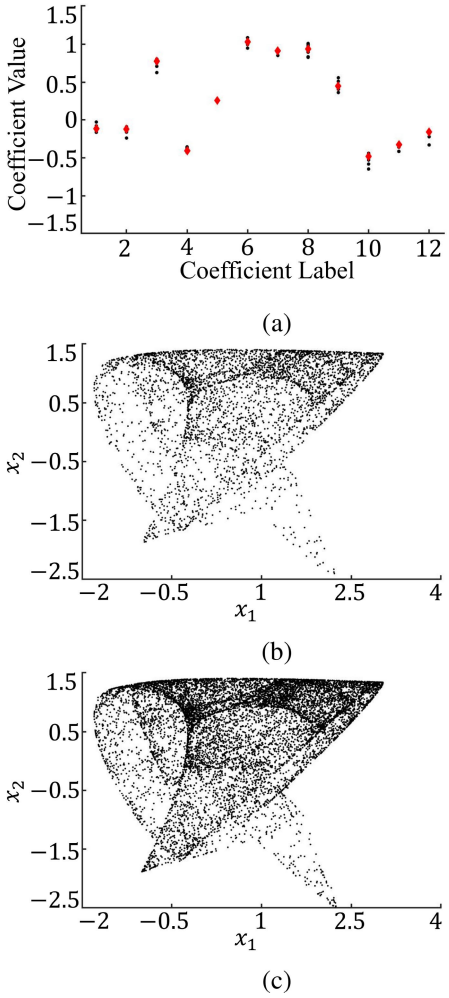

FIGURE 11. Optimal chaotic maps under uni-s weighting scheme, (a) system parameters of top 10 chaotic maps, the best is marked by red diamond, (b) phase portrait of best chaotic map, $L = 4000$, CD = 2.0489, $N_p = 2$, $D_{KY} = 2$, (c) phase portrait of best chaotic map, $L = 10000$, CD = 2.0387, $N_p = 2$, $D_{KY} = 2$.

Fig.16 shows the probability distribution of a regular sequence $x[\ell] = \mod(\ell - 1, 5) + 1$, with running-window size $d = 5$. Only five possible permutations emerge with equal probability, leading to PE = 0.336.

Fig.17 shows the probability distribution of permutation in $x_1[\ell]$ and $x_2[\ell]$, respectively, with sequence length of $L = 10000$ or $L = 4000$, under uni-s scheme.

The distributions are insensitive to the sequence length L. Fig.2 shows that the PE index is capped around 0.8. However, the optimal map under PE-s scheme can achieve PEs of 0.9495, 0.9409, comparable to 0.9744, 0.9807 in [4]. The high values of $N_p = 2$, $D_{KY} = 2$ and CD = 1.8273, as listed in Table 5, indicate a 2D strange attractor.

As summarized in Table 5, the optimal maps under weighting schemes uni-s, K-s and PE-s achieve CD $>$ 1.8, $K >$ 0.99, SE $>$ 0.9 and PE $>$ 0.8, making them suitable for image encryption. Fig.9(cs) shows 1D-like strange attractor

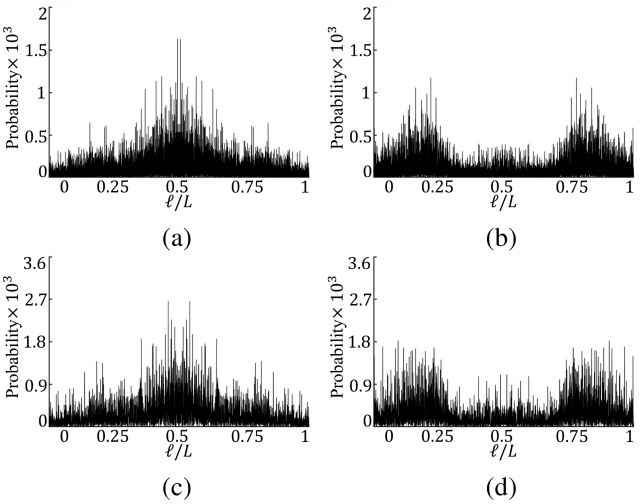

FIGURE 12. Probability (power spectrum) of (a) $x_1[\ell]$ and (b) $x_2[\ell]$, with $L = 10000$, (c) $x_1[\ell]$ and (d) $x_2[\ell]$, with Ł $= 4000$.

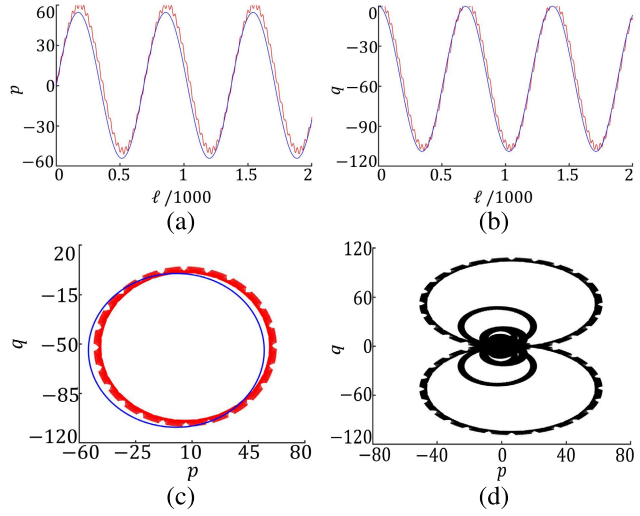

FIGURE 13. p and q sequences of $x[\ell] = \cos(c'_a \ell)$, with $c'_a = 0.11$ and $c_a = 0.1008$, (a) p sequence, ——: complete form, ——: approximate form in (12), (b) q sequence, ——: complete form, ——: approximate form in (13), (c) pq trace, ——: complete form, ——: approximate form in (12) and (13), (d) pq trace, $x[\ell] = \cos(c'_a \ell)$ with $1 \le \ell \le 10000$, $c_a = 2\pi(c_\ell/200)$ with $c_\ell = 1, 2, \cdots, 200$, $K = 0.0446$.

under SE-s scheme, associated with low CD of 1.53, losing some edge for image encryption.

III. IMAGE ENCRYPTION

The optimal chaotic maps acquired in the last Section are used to generate chaotic 2-sequences, which are then used to implement image encryption.

A. CRYPTOGRAPHY WITH HYBRID SEQUENCE GENERATION

Fig.18 shows the flow-chart of the proposed image encryption scheme, implemented with Algorithm 1. The hash values b_1 and b_2 are computed in step 1 and multiplied to the initial values $(x_1[1], x_2[1])$ in step 2 to enhance the resilience against

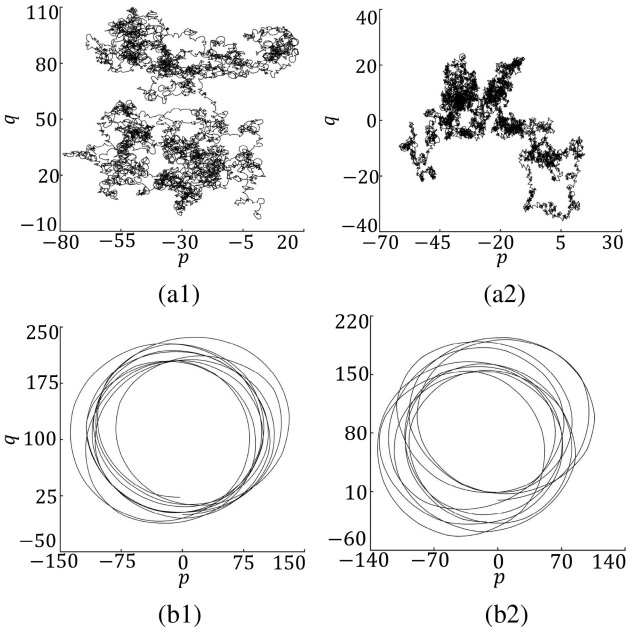

FIGURE 14. pq traces of $x_{1,2}[\ell']$ with $1 \le \ell' \le 10000$, under uni-s scheme, (a1) $x_1[\ell']$, $c_a = 2\pi(123/200)$, (a2) $x_2[\ell']$, $c_a = 2\pi(123/200)$, (b1) $x_1[\ell']$, $c_a = 2\pi(1/200)$, (b2) $x_2[\ell']$, $c_a = 2\pi(1/200)$.

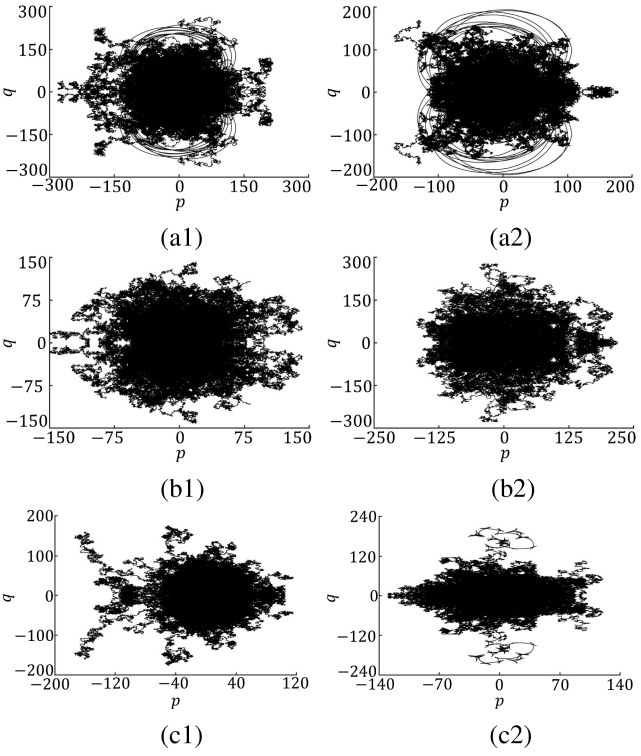

FIGURE 15. pq traces of $x_{1,2}[\ell']$ with $1 \le \ell' \le 10000$, $c_a = 2\pi(c_\ell/200)$ with $c_\ell = 1, 2, \cdots, 200$, (a1) $x_1[\ell']$ under uni-s scheme, $K = 0.9917$ (a2) $x_2[\ell']$ under uni-s scheme, $K = 0.9942$. (b1) $x_1[\ell']$ under K-s scheme, $K = 0.9970$ (b2) $x_2[\ell']$ under K-s scheme, $K = 0.9990$. p and q sequences of $x_{1,2}[\ell']$ with $1 \le \ell' \le 10000$ in [4], (c1) $x_1[\ell']$ in [4], $K = 0.9982$ (c2) $x_2[\ell']$ in [4], $K = 0.9965$.

differential attacks. In steps 3-5, 2-sequence $x_1[\ell]$ and $x_2[\ell]$ of length $L_m = \lceil \sqrt{3L_r L_c/2} \rceil$ are generated with initial values $(x_1[1], x_2[1])$ and chaotic-map system parameters $\{a_{nm_1m_2}\}$.

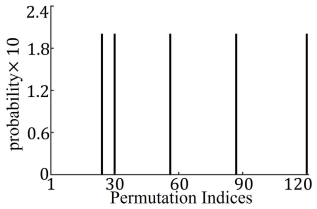

FIGURE 16. Probability distribution of a regular sequence $x[\ell] = \text{mod}\,(\ell - 1, 5) + 1$, with running-window size $d = 5$, PE = 0.336. Each permutation index indicates a specific permutation order, for example, index 1 corresponds to $x[\ell] \geq x[\ell + 1] \geq x[\ell + 2] \geq x[\ell + 3] \geq x[\ell + 4]$.

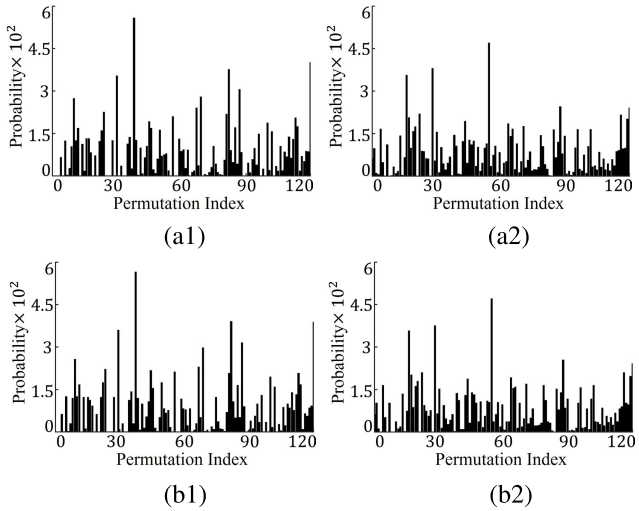

FIGURE 17. Probability distribution of permutation, under uni-s scheme, (a1) $x_1[\ell]$, $L = 10000$, PE = 0.8755, (a2) $x_2[\ell]$, $L = 10000$, PE = 0.9142, (b1) $x_1[\ell]$, $L = 4000$, PE = 0.8735, (b2) $x_2[\ell]$, $L = 4000$, PE = 0.9131.

In step 6, a hybrid sequence generation (HSG) method implemented with Algorithm 2 is proposed to generate a hybrid sequence $x_h[\ell]$. The HSG method is designed to save the encryption time by reducing the required sequence length since the generation of 2-sequences is time consuming. For an image of size (L_r, L_c, L_p), the required length of conventional 2-sequences is $L_r L_c L_p$, which is reduced to $\sqrt{3L_r L_c/2}$ by using the HSG method.

In step 7, a diffusion sequence $x_d[\ell]$ is generated. In step 8, the plaintext image $\mathcal{I}_p[\ell_r, \ell_c, \ell_p]$ is vectorized to a 1D array of $\mathcal{I}_{p1}[\ell]$. In step 9, $\mathcal{I}_{p1}[\ell]$ is permuted via $x_h[\ell]$ to acquire $\mathcal{I}'_{c1}[\ell]$. In step 10, $\mathcal{I}_{c1}[\ell]$ is obtained by applying XOR on $\mathcal{I}'_{c1}[\ell]$ and $x_d[\ell]$. In step 11, $\mathcal{I}_{c1}[\ell]$ is reformatted to a ciphertext image $\mathcal{I}_c[\ell_r, \ell_c, \ell_p]$.

Algorithm 2 shows the hybrid sequence generation (HSG) scheme to acquire a hybrid sequence $x_h[\ell]$. In step 1, 2D arrays $\tilde{x}_1[\ell_1, \ell_2]$ and $\tilde{x}_2[\ell_1, \ell_2]$, each of size $L_m \times L_m$, are generated in terms of the 2-sequences $x_1[\ell_1]$ and $x_2[\ell_2]$. In step 2, the two arrays $\tilde{x}_1[\ell_1, \ell_2]$ and $\tilde{x}_2[\ell_1, \ell_2]$ are vectorized into 1D arrays $\tilde{x}'_1[\ell]$ and $\tilde{x}'_2[\ell]$, respectively. In step 3, a hybrid sequence $x_h[\ell]$ of length $3L_r L_c$ is acquired by alternately copying the elements of $\tilde{x}'_1[\ell]$ and $\tilde{x}'_2[\ell]$.

Algorithm 3 shows the decryption scheme, which has the same architecture as the encryption scheme shown in Algorithm 1. Note that the diffusion operation is applied before permutation in the decryption scheme, while the order is reversed in the encryption scheme.

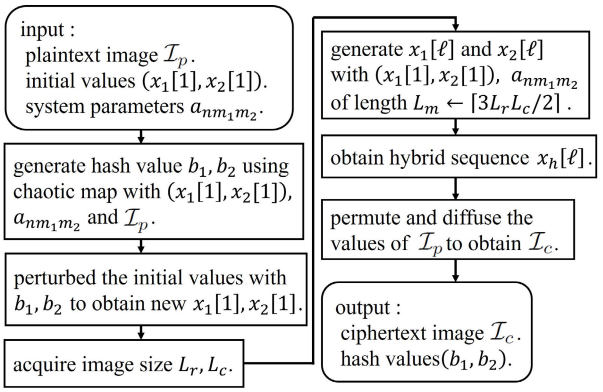

FIGURE 18. Flow-chart of image encryption scheme implemented with Algorithm 1.

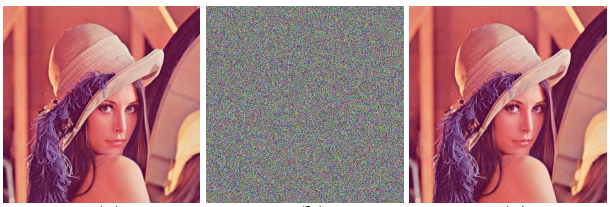

FIGURE 19. Demonstration of image encryption and decryption with optimal chaotic map under uni-s scheme, (a) plaintext image of Lenna, (b) encrypted image, (c) decrypted image.

B. ENCRYPTED IMAGES

Fig.19 demonstrates the results of image encryption and decryption with the optimal chaotic map under uni-s scheme. Fig.19(a) shows the plaintext image of Lenna, Figs.19(b) and 19(c) show the encrypted image and decrypted image, respectively. An ideal ciphertext image manifests random pixels, and the deciphertext image looks almost the same as the original plaintext image.

The information entropy (IE) is often used to measure the randomness of pixels in an image. Given a ciphertext image $\mathcal{I}_c[\ell_r, \ell_c, \ell_p]$, the occurrence rate (probability) $p[\ell_e]$ of pixel value $\ell_e - 1$, with $1 \leq \ell_e \leq 256$, is computed as

$$p[\ell_e] = \frac{1}{3L_rL_c} \sum_{\ell_r=1}^{L_r} \sum_{\ell_c=1}^{L_c} \sum_{\ell_p=1}^{3} Q(\mathcal{I}_c[\ell_r, \ell_c, \ell_p], \ell_e)$$

where

$$Q(\mathcal{I}, \ell_e) = \begin{cases} 1, & \mathcal{I} = \ell_e - 1 \\ 0, & \text{otherwise} \end{cases}$$

The information entropy is defined as

$$\text{IE} = -\sum_{\ell_e=1}^{256} p[\ell_e] \log_2 p[\ell_e]$$

Algorithm 1 Encryption Scheme

Input: plaintext image $\mathcal{I}_p$, initial values $(x_1[1], x_2[1])$, and system parameters $\{a_{nm_1m_2}\}$.

Output: ciphertext image $\mathcal{I}_c$, hash values (b_1, b_2).

Algorithm:

1) compute hash values b_1 and b_2.
   compute extended length L_e as
   $L_e = 2 \sum_{\ell_r,\ell_c,\ell_p} \mathcal{I}_p[\ell_r, \ell_c, \ell_p]$.
   compute $x_n[\ell]$ of length $L_e + 100$ with chaotic map of system parameters $\{a_{nm_1m_2}\}$ and initial values $(x_1[1], x_2[1])$.
   $x_{nf} = x_n[L_e + 100]$.
   $b_n = x_{nf},\ n = 1, 2$.
2) perturb the initial values as
   $x_n[1] \leftarrow x_n[1] + 0.1 \times x_n[1] \times x_{nf}, n = 1, 2$.
3) acquire image row number L_r and column number L_c.
4) $L_m = \lceil \sqrt{3L_rL_c/2} \rceil$
5) generate $x_1[\ell]$ and $x_2[\ell]$ of length L_m with chaotic map of system parameters $\{a_{nm_1m_2}\}$ and initial values $(x_1[1], x_2[1])$.
6) construct hybrid sequence $x_h[\ell]$, $1 \le \ell \le 3L_rL_c$, with Algorithm 2.
7) create diffusion sequence $x_d[\ell]$ as
   $x_d[\ell] \leftarrow \text{mod}\{\lfloor 10^5 x_h[\ell] \rfloor, 256\}$.
8) vectorize $\mathcal{I}_p[\ell_r, \ell_c, \ell_p]$ to $\mathcal{I}_{p1}[\ell]$, $1 \le \ell \le 3L_rL_c$.
   for $\ell_r = 1 : L_r$
    for $\ell_c = 1 : L_c$
     $\ell \leftarrow L_c(\ell_r - 1) + \ell_c$
     $\mathcal{I}_{p1}[\ell] \leftarrow \mathcal{I}_p[\ell_r, \ell_c, 1]$
     $\mathcal{I}_{p1}[L_rL_c + \ell] \leftarrow \mathcal{I}_p[\ell_r, \ell_c, 2]$
     $\mathcal{I}_{p1}[2L_rL_c + \ell] \leftarrow \mathcal{I}_p[\ell_r, \ell_c, 3]$
    end
   end
9) $\mathcal{I}'_{c1}[\ell] \leftarrow$ permute $\mathcal{I}_{p1}[\ell]$ with $x_h[\ell]$.
10) $\mathcal{I}_{c1}[\ell] \leftarrow \mathcal{I}'_{c1}[\ell] \oplus x_d[\ell]$.
11) generate ciphertext $\mathcal{I}_c[\ell_r, \ell_c, \ell_p]$.
   for $\ell_r = 1 : L_r$
    for $\ell_c = 1 : L_c$
     $k \leftarrow L_c(\ell_r - 1) + \ell_c$
     $\mathcal{I}_c[\ell_r, \ell_c, 1] \leftarrow \mathcal{I}_{c1}[k]$
     $\mathcal{I}_c[\ell_r, \ell_c, 2] \leftarrow \mathcal{I}_{c1}[L_rL_c + k]$
     $\mathcal{I}_c[\ell_r, \ell_c, 3] \leftarrow \mathcal{I}_{c1}[2L_rL_c + k]$
    end
   end

Algorithm 2 Hybrid Sequence Generation (HSG)

Input: 2-sequences $x_1[\ell]$ and $x_2[\ell]$, with $1 \le \ell \le L_m$, image size (L_r, L_c).

Output: hybrid sequence $x_h[\ell]$, with $1 \le \ell \le 3L_rL_c$.

Algorithm:

1) generate 2D arrays $\tilde{x}_1[\ell_1, \ell_2]$ and $\tilde{x}_2[\ell_1, \ell_2]$ of size $L_m \times L_m$.
   for $\ell_1 = 1 : L_m$
    for $\ell_2 = 1 : L_m$
     $\tilde{x}_1[\ell_1, \ell_2] = x_1[\ell_1] + x_2[\ell_2]$
     $\tilde{x}_2[\ell_1, \ell_2] = x_1[\ell_1] - x_2[\ell_2]$
    end
   end
2) vectorize $\tilde{x}_1[\ell_1, \ell_2]$ and $\tilde{x}_2[\ell_1, \ell_2]$ to $\tilde{x}'_1[\ell]$ and $\tilde{x}'_2[\ell]$, respectively, with $1 \le \ell \le L_m^2$.
   for $\ell_1 = 1 : L_m$
    for $\ell_2 = 1 : L_m$
     $\tilde{x}'_1[L_m(\ell_1 - 1) + \ell_2] = \tilde{x}_1[\ell_1, \ell_2]$
     $\tilde{x}'_2[L_m(\ell_1 - 1) + \ell_2] = \tilde{x}_2[\ell_1, \ell_2]$
    end
   end
3) generate hybrid sequence $x_h[\ell]$, with
   $x_h[1 : 2 : 3L_rL_c] \leftarrow \tilde{x}'_1[1 : \lceil (3L_rL_c - 1)/2 \rceil + 1]$
   $x_h[2 : 2 : 3L_rL_c] \leftarrow \tilde{x}'_2[1 : \lceil 3L_rL_c/2 \rceil]$

The maximum value of IE is 8, which is achieved with $p[\ell_e] = 1/256$ for $1 \le \ell_e \le 256$.

Fig.20 shows the histograms of the plaintext images and the ciphertext images, in red, green and blue channels, respectively, associated with the images shown in Fig.19. It is observed that the pixels in each color channel of the plaintext image follow a non-uniform distribution, while their counterparts in the ciphertext image follow a uniform distribution, indicating random pixels.

The values of adjacent pixels in a typical plaintext image are highly correlated, while those of an effective ciphertext image are highly uncorrelated. Given an image $\mathcal{I}[\ell_r, \ell_c, \ell_p]$ with size (L_r, L_c, L_p), correlation coefficients CR_h, CR_v and CR_d in the horizontal, vertical and diagonal directions, respectively, are determined as

$$\text{CR}_{ph} = \frac{\text{cov}(\mathcal{I}[\ell_r, \ell_c, \ell_p], \mathcal{I}[\ell_r, \ell_c + 1, \ell_p])}{\sigma(\mathcal{I}[\ell_r, \ell_c, \ell_p])\sigma(\mathcal{I}[\ell_r, \ell_c + 1, \ell_p])}$$

$$\text{CR}_{pv} = \frac{\text{cov}(\mathcal{I}[\ell_r, \ell_c, \ell_p], \mathcal{I}[\ell_r + 1, \ell_c, \ell_p]))}{\sigma(\mathcal{I}[\ell_r, \ell_c, \ell_p])\sigma(\mathcal{I}[\ell_r + 1, \ell_c, \ell_p])}$$

$$\text{CR}_{pd} = \frac{\text{cov}(\mathcal{I}[\ell_r, \ell_c, \ell_p], \mathcal{I}[\ell_r + 1, \ell_c + 1, \ell_p])}{\sigma(\mathcal{I}[\ell_r, \ell_c, \ell_p])\sigma(\mathcal{I}[\ell_r + 1, \ell_c + 1, \ell_p])}$$

where $\text{cov}(a, b)$ is the covariance between pixels a and b, and $\sigma(a)$ is the standard deviation of pixel a.

Table 7 lists the performance indices for image encryption, with the optimal chaotic maps under uni-s, K-s, SE-s and PE-s schemes, respectively. The information entropy of the ciphertext image generated with these four optimal chaotic maps is 7.9998, very close to the ideal value of 8. The maximum correlation coefficient among all three color channels and three directions is less than 4.7×10^{-3}, indicating the ciphertext images have pretty random pixels.

Algorithm 3 Decryption Scheme

Input: ciphertext image $\mathcal{I}_c$, initial values $(x_1[1], x_2[1])$, system parameters $\{a_{nm_1m_2}\}$ and hash values (b_1, b_2).

Output: deciphertext image $\mathcal{I}_d$

Algorithm:

1) perturb the initial condition
   $x_n[1] \leftarrow x_n[1] + 0.1 \times x_n[1] \times b_n,\ n = 1, 2.$
2) acquire row number L_r and column number L_c of image.
3) $L_m \leftarrow \lceil \sqrt{3L_rL_c/2} \rceil$
4) generate $x_1[\ell]$ and $x_2[\ell]$ of length L_m, by using chaotic map with system parameters $\{a_{nm_1m_2}\}$ and initial values $(x_1[1], x_2[1])$.
5) construct hybrid sequence $x_h[\ell]$, $1 \le \ell \le 3L_rL_c$ with Algorithm 2.
6) create diffusion sequence $x_d[\ell]$ as
   $x_d[\ell] \leftarrow \text{mod}\{\lfloor 10^5 x_h[\ell] \rfloor, 256\},\ n = 1, 2, 3.$
7) vectorize $\mathcal{I}_c[\ell_r, \ell_c, \ell_p]$ to $\mathcal{I}_{c1}[\ell]$, $1 \le \ell \le 3L_rL_c$.
   for $\ell_r = 1 : L_r$
    for $\ell_c = 1 : L_c$
     $\ell \leftarrow L_c(\ell_r - 1) + \ell_c$
     $\mathcal{I}_{c1}[\ell] \leftarrow \mathcal{I}_c[\ell_r, \ell_c, 1]$
     $\mathcal{I}_{c1}[L_rL_c + \ell] \leftarrow \mathcal{I}_c[\ell_r, \ell_c, 2]$
     $\mathcal{I}_{c1}[2L_rL_c + \ell] \leftarrow \mathcal{I}_c[\ell_r, \ell_c, 3]$
    end
   end
8) $\mathcal{I}'_{d1}[\ell] \leftarrow \mathcal{I}_{c1}[\ell] \oplus x_{d1}[\ell]$.
9) $\mathcal{I}_{d1}[\ell] \leftarrow$ permute $\mathcal{I}'_{d1}[\ell]$ with $x_h[\ell]$.
10) generate deciphertext $\mathcal{I}_d[\ell_r, \ell_c, \ell_p]$.
   for $\ell_r = 1 : L_r$
    for $\ell_c = 1 : L_c$
     $k \leftarrow L_c(\ell_r - 1) + \ell_c$
     $\mathcal{I}_d[\ell_r, \ell_c, 1] \leftarrow \mathcal{I}_{d1}[k]$
     $\mathcal{I}_d[\ell_r, \ell_c, 2] \leftarrow \mathcal{I}_{d1}[L_rL_c + k]$
     $\mathcal{I}_d[\ell_r, \ell_c, 3] \leftarrow \mathcal{I}_{d1}[2L_rL_c + k]$
    end
   end

C. RESILIENCE TO ATTACKS

Large key space provides more degrees of freedom to defend an encryption scheme against exhaustive attacks. The keys of encryption scheme derived from the proposed chaotic maps include 12 system parameters $\{a_{nm_1m_2}\}$ and two initial values $x_1[1], x_2[1]$. Each key is stored in a 64-bit word of IEEE754 standard [53], which is consisted of 1 sign bit, 11 exponent bits and 52 significant bits, attaining precision of $2^{-53} \simeq 1.11 \times 10^{-16}$. The key space is thus estimated on the precision of 10^{-15} as [4], [14], and [54] as $\log_2 10^{15\times(12+2)} \simeq 697$ bits.

Differential attacks are used to explore an encryption scheme for its system parameters and initial values, from the ciphertext images of two slightly different plaintext images. The encryption scheme is proven robust if the two ciphertext images resemble two random images without correlations.

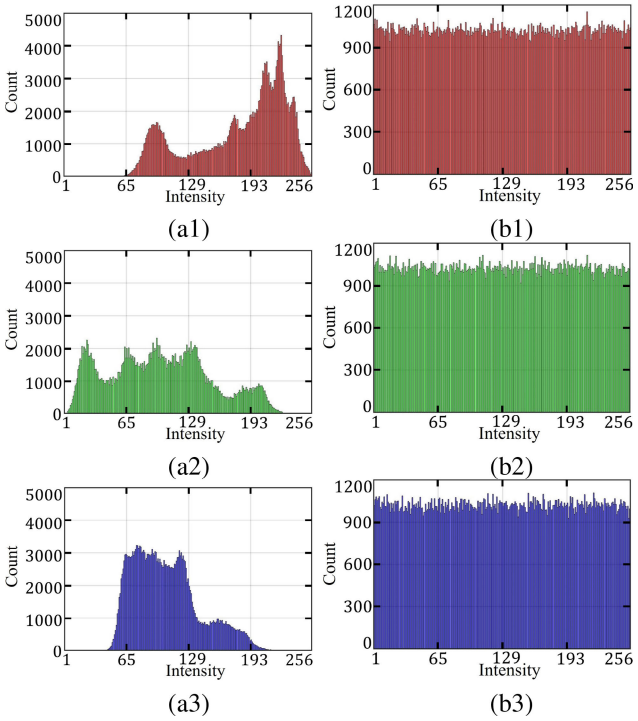

FIGURE 20. Histograms of plaintext images (a1, a2, a3) and ciphertext images (b1, b2, b3), where 1, 2 and 3 denote red, green and blue, respectively.

To be more specific, let the two slightly different plaintext images be $\mathcal{I}_p[\ell_r, \ell_c, \ell_p]$ and $\mathcal{I}'_p[\ell_r, \ell_c, \ell_p]$, and their ciphertext images be $\mathcal{I}_c[\ell_r, \ell_c, \ell_p]$ and $\mathcal{I}'_c[\ell_r, \ell_c, \ell_p]$, respectively. The difference between the two ciphertext images is quantified in terms of a number-of-pixel change rate (NPCR) as [13]

$$\text{NPCR} = \frac{1}{3L_rL_c} \sum_{\ell_r=r}^{L_r} \sum_{\ell_c=1}^{L_c} \sum_{\ell_p=1}^{3} D(\ell_r, \ell_c, \ell_p)$$

with

$$D(\ell_r, \ell_c, \ell_p) = \begin{cases} 1, & \mathcal{I}_c[\ell_r, \ell_c, \ell_p] = \mathcal{I}'_c[\ell_r, \ell_c, \ell_p] \\ 0, & \mathcal{I}_c[\ell_r, \ell_c, \ell_p] \neq \mathcal{I}'_c[\ell_r, \ell_c, \ell_p] \end{cases}$$

and a unified average changing intensity (UACI) as [13]

$$\text{UACI} = \frac{1}{3L_rL_c \times 255} \sum_{\ell_r=r}^{L_r} \sum_{\ell_c=1}^{L_c} \sum_{\ell_p=1}^{3} |\mathcal{I}_c[\ell_r, \ell_c, \ell_p) - \mathcal{I}'_c(\ell_r, \ell_c, \ell_p)|$$

The NPCR gives the proportion of affected pixels in a ciphertext image if one bit of the plaintext image is changed. The probability for two 8-bit random numbers in [0, 255] to be the same is $1/256 \simeq 0.39\%$, which implies the highest value of NPCR is $\simeq 99.61\%$. The UACI measures the change of pixel values. By picking two bytes from a uniform distribution in [0, 255], the expectation value of the absolute difference between these two bytes is 85.33, which implies

TABLE 7. Performance indices for image encryption.

model	key space	IE	NPCR	UACI
uni-s	697	7.9998	99.61 %	33.46 %
K-s	697	7.9998	99.61 %	33.45 %
SE-s	697	7.9998	99.61 %	33.48 %
PE-s	697	7.9998	99.61 %	33.47 %
model	$\mathrm{CR}_{rh} \times 10^4$	$\mathrm{CR}_{rv} \times 10^4$	$\mathrm{CR}_{rd} \times 10^4$	
uni-s	42	-17	23	
K-s	13	23	-2.0	
SE-s	6.9	46	34	
PE-s	30	-24	-6.1	
model	$\mathrm{CR}_{gh} \times 10^4$	$\mathrm{CR}_{gv} \times 10^4$	$\mathrm{CR}_{gd} \times 10^4$	
uni-s	-5.8	4.3	-30	
K-s	-6	-20	2.6	
SE-s	-19	16	-18	
PE-s	7.2	6.0	0.74	
model	$\mathrm{CR}_{bh} \times 10^4$	$\mathrm{CR}_{bv} \times 10^4$	$\mathrm{CR}_{bd} \times 10^4$	
uni-s	-24	-6.3	-1.8	
K-s	-24	-12	-8.8	
SE-s	-24	12	-18	
PE-s	13	7.4	-1.1	

the highest value of UACI is $85.33/255 = 33.46\%$. In [54], a statistical approach was used to derive the values of NPCR and UACI as 99.57% and 33.28%, respectively, for an image of size $512 \times 512 \times 3$.

TABLE 8. NPCR and UACI between $\mathcal{I}_c$ and $\mathcal{I}'_c$, R: image with random pixels, P: plaintext image of Lenna.

factor	$\mathcal{I}_c$	$\mathcal{I}'_c$	value
NPCR	R	R	99.61 %
NPCR	R	P	99.61 %
UACI	R	R	33.46 %
UACI	R	P	30.42 %

Table 8 lists the values of NPCR and UACI between $\mathcal{I}_c$ and $\mathcal{I}'_c$, where R and P refer to plaintext images of random pixels and Lenna, respectively, $\mathcal{I}_c$ is encrypted from image R and $\mathcal{I}'_c$ is encrypted from image R or P. The NPCR between $\mathcal{I}_c$ and $\mathcal{I}'_c$ sustains 99.61% with $\mathcal{I}'_c$ encrypted from R or P. The UACI is 30.42 % if $\mathcal{I}'_c$ is encrypted from P, 33.46% if $\mathcal{I}'_c$ is encrypted from R, because adjacent pixels in image P have higher correlation than those in image R.

A robust chaotic-map encryption scheme should have high key sensitivity [37], [55], [56], which means a plaintext image will not be recoverable even if an encryption key is slightly perturbed. To test the key sensitivity of the proposed chaotic-map encryption scheme, we first flip the least significant bit of one key, among 12 system parameters $a_{nm_1m_2}$'s and two initial values $x_1[1]$, $x_2[1]$, then compute the number-of-pixel change rate (NPCR_K) and the unified average changing intensity (UACI_K) between the plaintext image and the decrypted image, similar to the number-of-bit change rate in [57]. The subscript K in NPCR_K and UACI_K indicates these two factors are used specifically to evaluate the key sensitivity. If the decrypted image after flipping the least significant bit of a key manifests random pixels, the key sensitivity is proven high.

TABLE 9. NPCR_K with least significant bit of key flipped.

perturbed key	uni-s	K-s	SE-s	PE-s
$x_1[1]$	0	99.62 %	99.60 %	99.61 %
$x_2[1]$	0	99.62 %	99.61 %	99.61 %
a_{100}	99.60 %	99.62 %	99.61 %	99.61 %
a_{110}	99.60 %	99.61 %	99.60 %	99.61 %
a_{101}	99.60 %	99.60 %	99.60 %	99.61 %
a_{120}	99.60 %	99.60 %	99.61 %	99.61 %
a_{111}	99.62 %	99.61 %	99.62 %	99.61 %
a_{102}	99.60 %	99.60 %	99.60 %	99.60 %
a_{200}	99.60 %	99.60 %	99.61 %	99.62 %
a_{210}	99.61 %	99.61 %	99.61 %	99.60 %
a_{201}	99.62 %	99.60 %	99.61 %	99.61 %
a_{220}	99.61 %	99.61 %	99.61 %	99.62 %
a_{211}	99.61 %	99.60 %	99.61 %	99.61 %
a_{202}	99.59 %	99.60 %	99.61 %	99.61 %

TABLE 10. UACI_K with least significant bit of key flipped.

perturbed key	uni-s	K-s	SE-s	PE-s
$x_1[1]$	0 %	30.45 %	30.44 %	30.44 %
$x_2[1]$	0 %	30.45 %	30.43 %	30.41 %
a_{100}	30.43 %	30.45 %	30.46 %	30.40 %
a_{110}	30.39 %	30.38 %	30.46 %	30.47 %
a_{101}	30.42 %	30.47 %	30.44 %	30.45 %
a_{120}	30.46 %	30.43 %	30.46 %	30.40 %
a_{111}	30.45 %	30.45 %	30.45 %	30.47 %
a_{102}	30.40 %	30.43 %	30.42 %	30.37 %
a_{200}	30.46 %	30.39 %	30.45 %	30.44 %
a_{210}	30.41 %	30.41 %	30.42 %	30.43 %
a_{201}	30.37 %	30.47 %	30.41 %	30.47 %
a_{220}	30.41 %	30.46 %	30.41 %	30.42 %
a_{211}	30.47 %	30.39 %	30.45 %	30.43 %
a_{202}	30.44 %	30.41 %	30.42 %	30.43 %

Tables 9 and 10 list the NPCR_K and UACI_K, respectively, by flipping the least significant bit of a key. Chaotic maps under K-s, SE-s and PE-s weighting schemes manifest high key sensitivity, with NPCR_K and UACI_K close to 99.61 % and 30.42 %, respectively, indicating the decrypted images appear random. The key sensitivity to the two initial values $x_1[1]$, $x_2[1]$ of chaotic map under uni-s scheme is zero, when the least significant bit is flipped.

Tables 11 and 12 list the NPCR_K and UACI_K, respectively, with the third least significant bit of a key flipped. As the variation of key is increased, all the values of NPCR_K and UACI_K are close to 99.61 % and 30.42 %, respectively, with chaotic maps under four different weighting schemes.

Figs.21(a), 21(b) and 21(c) show the decrypted images by flipping the third least significant bit of key parameters $x_1[1]$, a_{120} and a_{111}, respectively, under uni-s weighting scheme. All these three decrypted images manifest random pixels, confirming high key sensitivity.

A structural similarity index measure (SSIM) has been used to evaluate the similarity between two images $\mathcal{I}_1$ and

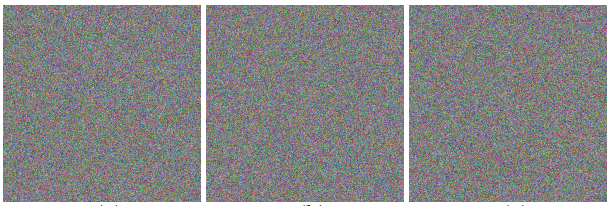

FIGURE 21. Decrypted images by flipping the third least significant bit of a key under uni-s weighting scheme, (a) $x_1[1]$, (b) a_{120}, (c) a_{111}.

TABLE 11. NPCR_K with third least significant bit of key flipped.

perturbed key	uni-s	K-s	SE-s	PE-s
$x_1[1]$	99.61 %	99.61 %	99.62 %	99.61 %
$x_2[1]$	99.61 %	99.62 %	99.60 %	99.60 %
a_{100}	99.62 %	99.60 %	99.61 %	99.61 %
a_{110}	99.61 %	99.61 %	99.61 %	99.60 %
a_{101}	99.61 %	99.61 %	99.60 %	99.60 %
a_{120}	99.61 %	99.60 %	99.62 %	99.61 %
a_{111}	99.60 %	99.61 %	99.61 %	99.62 %
a_{102}	99.61 %	99.61 %	99.60 %	99.61 %
a_{200}	99.62 %	99.60 %	99.61 %	99.61 %
a_{210}	99.60 %	99.61 %	99.61 %	99.60 %
a_{201}	99.61 %	99.61 %	99.61 %	99.60 %
a_{220}	99.61 %	99.61 %	99.61 %	99.61 %
a_{211}	99.61 %	99.60 %	99.60 %	99.60 %
a_{202}	99.62 %	99.61 %	99.61 %	99.61 %

$\mathcal{I}_2$ as [58]

$$\text{SSIM}(\mathcal{I}_1, \mathcal{I}_2) = \text{Lu}(\mathcal{I}_1, \mathcal{I}_2) C(\mathcal{I}_1, \mathcal{I}_2) S(\mathcal{I}_1, \mathcal{I}_2)$$

with

$$\text{Lu}(\mathcal{I}_1, \mathcal{I}_2) = \frac{2\mu_1\mu_2 + c_1}{\mu_1^2 + \mu_2^2 + c_1}$$
$$C(\mathcal{I}_1, \mathcal{I}_2) = \frac{2\sigma_1\sigma_2 + c_2}{\sigma_1^2 + \sigma_2^2 + c_2}$$
$$S(\mathcal{I}_1, \mathcal{I}_2) = \frac{2\sigma_{12} + c_2}{2\sigma_1\sigma_2 + c_2}$$

where Lu, C and S delineate the similarity on luminance, contrast and structure, respectively, μ_n and σ_n are the mean and variance, respectively, of pixels in image $\mathcal{I}_n$, σ_{12} is the covariance of pixels between images $\mathcal{I}_1$ and $\mathcal{I}_2$, $c_1 = (0.01 \times 255)^2$ and $c_2 = (0.03 \times 255)^2$ are empirical coefficients tried out in this work.

Fig.22 shows the resilience to occlusion attacks of the optimal chaotic map under uni-s scheme. The ciphertext image is blocked by 20%, 50% and 80%, respectively, in image area or pixel number. It is observed that the decrypted image is still discernible if the ciphertext image is blocked by less than 80%.

Fig.23 shows that the SSIM between the plaintext image and the decrypted image, with the optimal chaotic map under uni-s scheme, drops almost linearly as the blocking percentage increases.

TABLE 12. UACI_K with third least significant bit of key flipped.

perturbed key	uni-s	K-s	SE-s	PE-s
$x_1[1]$	30.39 %	30.45 %	30.43 %	30.44 %
$x_2[1]$	30.41 %	30.44 %	30.41 %	30.43 %
a_{100}	30.42 %	30.42 %	30.48 %	30.42 %
a_{110}	30.43 %	30.43 %	30.40 %	30.43 %
a_{101}	30.39 %	30.45 %	30.45 %	30.44 %
a_{120}	30.41 %	30.42 %	30.42 %	30.44 %
a_{111}	30.43 %	30.45 %	30.42 %	30.41 %
a_{102}	30.39 %	30.43 %	30.43 %	30.43 %
a_{200}	30.44 %	30.42 %	30.43 %	30.47 %
a_{210}	30.43 %	30.44 %	30.46 %	30.43 %
a_{201}	30.37 %	30.39 %	30.42 %	30.45 %
a_{220}	30.38 %	30.46 %	30.41 %	30.40 %
a_{211}	30.40 %	30.41 %	30.49 %	30.42 %
a_{202}	30.46 %	30.45 %	30.48 %	30.43 %

FIGURE 22. Resilience to occlusion attacks of optimal chaotic map under uni-s scheme, (a1) ciphertext blocked by 20 %, (b1) ciphertext blocked by 50 %, (c1) ciphertext blocked by 80 %, (a2) decrypted image from (a1), (b2) decrypted image from (b1), (c2) decrypted image from (c1).

D. CPU TIME FOR SEQUENCE GENERATION AND IMAGE ENCRYPTION

Fig.24 shows the CPU time for generating 2-sequences of length L with the proposed method and various chaotic maps in the literature. The CPU time is dominated by the number of multiplications and divisions used to implement the

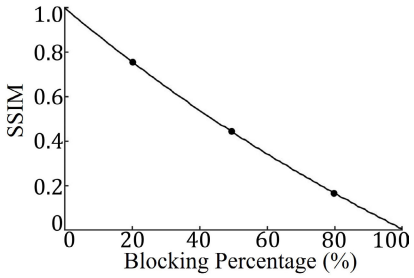

FIGURE 23. SSIM versus blocking percentage with optimal chaotic map under uni-s scheme, • marks the cases shown in Fig.22.

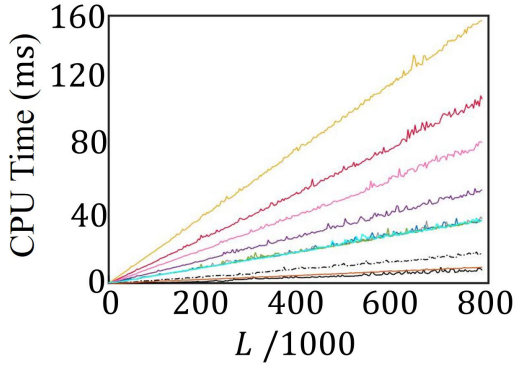

FIGURE 24. CPU time for generating 2-sequences of length L. ———: hybrid of short 2-sequences from 2D chaotic map of order 2, – – –: 2D chaotic map of order 2, ———: Henon map [10], ———: Zeraoulia Sprott map [10], ———: Duffing map [10], ———: 2D non-invertible chaotic economic map [14], ———: 2D-OPMAP [23], ———: memristor-coupled logistic map [13], ———: 2D sine map [26], ———: 2D-SCMCI hyperchaotic map [4], ———: 2D memristive map [2].

chaotic maps. The 2D-OPMAP [23] takes 12 multiplications and 2 mod functions to generate each element of the 2-sequences, with each mod function taking one division and one multiplication. The 2D non-invertible chaotic economic map [14] takes 8 multiplications to generate one element. In this work, the CPU time to calculate $\bar{x}[\ell]$ from $\bar{x}[\ell-1]$ as in (2) is independent of ℓ, thus the total CPU time is a linear function of L. The chaotic map in (5) and (6) takes 10 multiplications. Without using the hybrid sequence generation method, the required sequence generation time will be longer than that in [14].

The image encryption time is the sum of sequence generation time to create chaotic sequences and image confusion time to transform a plaintext image to an encrypted image by using the chaotic sequences. This work mainly focuses on reducing the sequence generation time. By applying the proposed hybrid sequence generation method in Algorithm 2, the sequence generation time is reduced from 0.017 s to 0.0074 s with $L = 512 \times 512 \times 3$. The image encryption time is reduced from 0.0574 s to 0.0478 s, as listed in Table 2, along with other methods in the literature.

E. HIGHLIGHT OF NOVELTY AND CONTRIBUTIONS

The novelty and contributions of this work are summarized as follows.

1) A genre of second-order chaotic maps is proposed for high-security image encryption. Candidates of chaotic map are screened with a weak condition and a strong condition, respectively, in terms of six complexity indices. The strong screening condition expedites the preparation of candidates for optimization.
2) A particle swarm optimization (PSO) algorithm is developed to fine-tune the chaotic maps through different weighting schemes on the complexity indices of N_p, D_{KY}, CD, K, PE and SE. Eight different optimal chaotic maps are acquired effectively and quickly, with four under weak screening condition and four under strong screening condition. These chaotic maps achieve $K \geq 0.9$, SE ≥ 0.9, PE ≥ 0.7, better than most counterparts in the literature.
3) The proposed image encryption method achieves a key space of 697 bits, correlation coefficients of ciphertext images below 4.7×10^{-3}, information entropy of 7.9997, NPCR of 99.61% and UACI of 33.46%. The proposed hybrid sequences generated with 2D chaotic maps of order 2 can significantly reduce the CPU time required for generating chaotic sequences.

Initially, a large number of chaotic-map candidates are generated under the limited range and possible discontinuity of system parameters. It takes about 1.5 CPU hours to collect 300 chaotic-map candidates under weak condition in (7) and about 3 CPU hours under strong condition in (8). By simulations, there are about 2 candidates out of 300 that generate divergent chaotic sequences under (8). The optimal chaotic map under the SE-s weighting scheme is more probable to generate divergent chaotic sequences compared with the other weighting schemes.

IV. CONCLUSION

Second-order chaotic maps with random coefficients have been systematically analyzed in terms of six complexity indices. Two screening conditions are proposed to establish initial population of candidate maps more effectively, expedite the optimization of chaotic maps, and achieve the highest possible complexity of the generated 2-sequences. The system parameters thus acquired have continuous range and much larger key space, making them suitable for image encryption. Eight different optimal chaotic maps are generated from four sets of weighting coefficients in the objective function and two sets of chaotic-map candidates. The chaotic sequences generated with the optimal chaotic maps achieve $K \geq 0.9$, SE ≥ 0.9, PE ≥ 0.7, better than their counterparts in the literature.

A hybrid sequence generation (HSG) method is proposed to reduce the image encryption time from 0.0574 s to 0.0478 s. The ciphertext images are close to random

images, with information entropy IE $>$ 7.99975 and correlation coefficients $<$ 4.7×10^{-3}. The proposed image encryption scheme is robust against differential attacks, with NPCR $\sim$ 99.61% and UACI $\sim$ 33.46%. High key sensitivity is proven by flipping the least significant bit of the 12 system parameters and two initial values, respectively.

REFERENCES

[1] J. L. Kaplan and J. A. York, "Chaotic behavior of multidimensional difference equations," *Functional Differential Equations and Approximations of Fixed Points*, (Lecture Notes in Mathematics), vol. 730, H. O. Peitgen and H. O. Walter, Eds. Berlin, Germany: Springer, 1979.

[2] Q. Lai and C. Lai, "Design and implementation of a new hyperchaotic memristive map," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 4, pp. 2331–2335, Apr. 2022, doi: 10.1109/TCSII.2022.3151802.

[3] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd ed. the University of Michigan, Avalon Publishing, 1989, pp. 268–269.

[4] J. Sun, "2D-SCMCI hyperchaotic map for image encryption algorithm," *IEEE Access*, vol. 9, pp. 59313–59327, 2021, doi: 10.1109/ACCESS.2021.3070350.

[5] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, Jun. 1976, doi: 10.1038/261459a0.

[6] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963, doi: 10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

[7] M. Hénon, "A two-dimensional mapping with a strange attractor," *Commun. Math. Phys.*, vol. 50, no. 1, pp. 69–77, Feb. 1976, doi: 10.1007/BF01608556.

[8] M. S. Shabbir, Q. Din, R. Alabdan, A. Tassaddiq, and K. Ahmad, "Dynamical complexity in a class of novel discrete-time predator-prey interaction with cannibalism," *IEEE Access*, vol. 8, pp. 100226–100240, 2020, doi: 10.1109/ACCESS.2020.2995679.

[9] J. S. Muthu and P. Murali, "Review of chaos detection techniques performed on chaotic maps and systems in image encryption," *Social Netw. Comput. Sci.*, vol. 2, no. 5, p. 392, Sep. 2021, doi: 10.1007/s42979-021-00778-3.

[10] Z. Hua, Y. Zhang, and Y. Zhou, "Two-dimensional modular chaotification system for improving chaos complexity," *IEEE Trans. Signal Process.*, vol. 68, pp. 1937–1949, 2020, doi: 10.1109/TSP.2020.2979596.

[11] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 6, pp. 3713–3724, Jun. 2021, doi: 10.1109/TSMC.2019.2932616.

[12] J. Gu, C. Li, Y. Chen, H. H. C. Iu, and T. Lei, "A conditional symmetric memristive system with infinitely many chaotic attractors," *IEEE Access*, vol. 8, pp. 12394–12401, 2020, doi: 10.1109/ACCESS.2020.2966085.

[13] B. Bao, K. Rong, H. Li, K. Li, Z. Hua, and X. Zhang, "Memristor-coupled logistic hyperchaotic map," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 8, pp. 2992–2996, Aug. 2021, doi: 10.1109/TCSII.2021.3072393.

[14] A. A. Karawia and Y. A. Elmasry, "New encryption algorithm using bit-level permutation and non-invertible chaotic map," *IEEE Access*, vol. 9, pp. 101357–101368, 2021, doi: 10.1109/ACCESS.2021.3096995.

[15] S. Vaidyanathan, A. Sambas, E. Tlelo-Cuautle, A. A. A. El-Latif, B. Abd-El-Atty, O. Guillén-Fernández, K. Benkouider, M. A. Mohamed, M. Mamat, and M. A. H. Ibrahim, "A new 4-D multi-stable hyperchaotic system with no balance point: Bifurcation analysis, circuit simulation, FPGA realization and image cryptosystem," *IEEE Access*, vol. 9, pp. 144555–144573, 2021, doi: 10.1109/ACCESS.2021.3121428.

[16] H. Zhang, X. Wang, H. Xie, C. Wang, and X. Wang, "An efficient and secure image encryption algorithm based on non-adjacent coupled maps," *IEEE Access*, vol. 8, pp. 122104–122120, 2020, doi: 10.1109/ACCESS.2020.3006513.

[17] X. Wang and P. Liu, "A new image encryption scheme based on a novel one-dimensional chaotic system," *IEEE Access*, vol. 8, pp. 174463–174479, 2020, doi: 10.1109/ACCESS.2020.3024869.

[18] W. Marszalek, M. Walczak, and J. Sadecki, "Two-parameter 0–1 test for chaos and sample entropy bifurcation diagrams for nonlinear oscillating systems," *IEEE Access*, vol. 9, pp. 22679–22687, 2021, doi: 10.1109/ACCESS.2021.3055715.

[19] X. Du, L. Wang, D. Yan, and S. Duan, "A multiring Julia fractal chaotic system with separated-scroll attractors," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 12, pp. 2210–2219, Dec. 2021, doi: 10.1109/TVLSI.2021.3106312.

[20] H. Li, H. Bao, L. Zhu, B. Bao, and M. Chen, "Extreme multistability in simple area-preserving map," *IEEE Access*, vol. 8, pp. 175972–175980, 2020, doi: 10.1109/ACCESS.2020.3026676.

[21] S. He, K. Sun, and S. Banerjee, "Dynamical properties and complexity in fractional-order diffusionless Lorenz system," *Eur. Phys. J. Plus*, vol. 131, no. 8, pp. 1–12, Aug. 2016, doi: 10.1140/epjp/i2016-16254-8.

[22] C. Bandt and B. Pompe, "Permutation entropy: A natural complexity measure for time series," *Phys. Rev. Lett.*, vol. 88, no. 17, Apr. 2002, Art. no. 174102, doi: 10.1103/PhysRevLett.88.174102.

[23] A. Toktas, U. Erkan, F. Toktas, and Z. Yetgin, "Chaotic map optimization for image encryption using triple objective differential evolution algorithm," *IEEE Access*, vol. 9, pp. 127814–127832, 2021, doi: 10.1109/ACCESS.2021.3111691.

[24] Z. Elhadj and J. C. Sprott, "On the dynamics of a new simple 2-D rational discrete mapping," *Int. J. Bifurcation Chaos*, vol. 21, no. 1, pp. 155–160, Jan. 2011.

[25] A. Mahdi, A. K. Jawad, and S. S. Hreshee, "Digital chaotic scrambling of voice based on duffing map," *Int. J. Inf. Commun. Sci. Commun.*, vol. 1, no. 2, pp. 16–21, 2016.

[26] H. Bao, Z. Hua, N. Wang, L. Zhu, M. Chen, and B. Bao, "Initials-boosted coexisting chaos in a 2-D sine map and its hardware implementation," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1132–1140, Feb. 2021, doi: 10.1109/TII.2020.2992438.

[27] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017, doi: 10.1016/j.optlaseng.2016.08.009.

[28] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-sine map and DNA approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018, doi: 10.1016/j.sigpro.2018.06.008.

[29] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018, doi: 10.1016/j.sigpro.2017.08.020.

[30] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 7, pp. 4402–4414, Jul. 2022, doi: 10.1109/TSMC.2021.3096967.

[31] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Jun. 1998.

[32] J. Sun, C. Li, T. Lu, A. Akgul, and F. Min, "A memristive chaotic system with hypermultistability and its application in image encryption," *IEEE Access*, vol. 8, pp. 139289–139298, 2020, doi: 10.1109/ACCESS.2020.3012455.

[33] X. Wang and P. Liu, "A new full chaos coupled mapping lattice and its application in privacy image encryption," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 3, pp. 1291–1301, Mar. 2022, doi: 10.1109/TCSI.2021.3133318.

[34] Y. Zhang, H. Xiang, S. Zhang, and L. Liu, "Construction of high-dimensional cyclic symmetric chaotic map with one-dimensional chaotic map and its security application," *Multimedia Tools Appl.*, vol. 82, no. 12, pp. 17715–17740, May 2023, doi: 10.1007/s11042-022-14044-y.

[35] Z. Hua, Y. Zhang, H. Bao, H. Huang, and Y. Zhou, "N-dimensional polynomial chaotic system with applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 2, pp. 784–797, Feb. 2022, doi: 10.1109/TCSI.2021.3117865.

[36] W. Cao, H. Cai, and Z. Hua, "N-dimensional chaotic map with application in secure communication," *Chaos, Solitons Fractals*, vol. 163, Oct. 2022, Art. no. 112519, doi: 10.1016/j.chaos.2022.112519.

[37] H. Li, T. Li, W. Feng, J. Zhang, J. Zhang, L. Gan, and C. Li, "A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102844, doi: 10.1016/j.jisa.2021.102844.

[38] W. Feng, X. Zhao, J. Zhang, Z. Qin, J. Zhang, and Y. He, "Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform," *Mathematics*, vol. 10, no. 15, p. 2751, Aug. 2022, doi: 10.3390/math10152751.

[39] K. Qian, W. Feng, Z. Qin, J. Zhang, X. Luo, and Z. Zhu, "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," *Frontiers Phys.*, vol. 10, Aug. 2022, Art. no. 963795, doi: 10.3389/fphy.2022.963795.

[40] X. Wang and P. Liu, "Image encryption based on roulette cascaded chaotic system and alienated image library," *Vis. Comput.*, vol. 38, no. 3, pp. 763–779, Mar. 2022, doi: 10.1007/s00371-020-02048-4.
[41] W. Feng, Z. Qin, J. Zhang, and M. Ahmad, "Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding," *IEEE Access*, vol. 9, pp. 145459–145470, 2021, doi: 10.1109/ACCESS.2021.3123571.
[42] W. Feng and J. Zhang, "Cryptanalzing a novel hyper-chaotic image encryption scheme based on pixel-level filtering and DNA-level diffusion," *IEEE Access*, vol. 8, pp. 209471–209482, 2020, doi: 10.1109/ACCESS.2020.3038006.
[43] W. Feng, Y.-G. He, H.-M. Li, and C.-L. Li, "Cryptanalysis of the integrated chaotic systems based image encryption algorithm," *Optik*, vol. 186, pp. 449–457, Jun. 2019, doi: 10.1016/j.ijleo.2018.12.103.
[44] P. Liu, X. Wang, Y. Su, H. Liu, and S. Unar, "Globally coupled private image encryption algorithm based on infinite interval spatiotemporal chaotic system," *IEEE Trans. Circuits Syst. I*, vol. 70, no. 6, pp. 2511–2522, Jun. 2023, doi: 10.1109/TCSI.2023.3250713.
[45] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021, doi: 10.1016/j.ins.2020.09.055.
[46] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, B. Abd-El-Atty, A. A. A. El-Latif, O. Guillén-Fernández, Y. Hidayat, and G. Gundara, "A 3-D multi-stable system with a peanut-shaped equilibrium curve: Circuit design, FPGA realization, and an application to image encryption," *IEEE Access*, vol. 8, pp. 137116–137132, 2020, doi: 10.1109/ACCESS.2020.3011724.
[47] H. Lin, C. Wang, F. Yu, C. Xu, Q. Hong, W. Yao, and Y. Sun, "An extremely simple multiwing chaotic system: Dynamics analysis, encryption application, and hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 68, no. 12, pp. 12708–12719, Dec. 2021, doi: 10.1109/TIE.2020.3047012.
[48] W. K. Chen, *The Circuits and Filters Handbook*. Boca Raton, FL, USA: CRC Press, 2002. [Online]. Available: https://books.google.com.tw/books?id=SmDImt1zHXkC
[49] I. Ahmad and B. Srisuchinwong, "Simple chaotic jerk flows with families of self-excited and hidden attractors: Free control of amplitude, frequency, and polarity," *IEEE Access*, vol. 8, pp. 46459–46471, 2020, doi: 10.1109/ACCESS.2020.2978660.
[50] S. Zhang, C. Li, J. Zheng, X. Wang, Z. Zeng, and X. Peng, "Generating any number of initial offset-boosted coexisting Chua's double-scroll attractors via piecewise-nonlinear memristor," *IEEE Trans. Ind. Electron.*, vol. 69, no. 7, pp. 7202–7212, Jul. 2022, doi: 10.1109/TIE.2021.3099231.
[51] A. Douady and J. Oesterle, "Dimension de Hausdorff des attracteurs," *CR Acad. Sc. Paris*, vol. 290, pp. 1135–1138, Sep. 1980.
[52] G. A. Gottwald and I. Melbourne, "The 0–1 test for chaos: A review," *Chaos Detection and Predictability* (Lecture Notes in Physics), vol. 915, C. Skokos, G. Gottwald, and J. Laskar, Eds. Berlin, Germany: Springer, 2016, doi: 10.1007/978-3-662-48410-4_7.
[53] *IEEE Standard for Floating-Point Arithmetic*, IEEE Standard 754-2019 (Revision IEEE 754-2008), pp. 1–84, Jul. 2019, doi: 10.1109/IEEESTD.2019.8766229.
[54] J. Hao, H. Li, H. Yan, and J. Mou, "A new fractional chaotic system and its application in image encryption with DNA mutation," *IEEE Access*, vol. 9, pp. 52364–52377, 2021, doi: 10.1109/ACCESS.2021.3069977.
[55] W. Feng, Y. He, H. Li, and C. Li, "A plain-image-related chaotic image encryption algorithm based on DNA sequence operation and discrete logarithm," *IEEE Access*, vol. 7, pp. 181589–181609, 2019, doi: 10.1109/ACCESS.2019.2959137.
[56] W. Feng, Y.-G. He, H.-M. Li, and C.-L. Li, "Image encryption algorithm based on discrete logarithm and memristive chaotic system," *Eur. Phys. J. Special Topics*, vol. 228, no. 10, pp. 1951–1967, Oct. 2019, doi: 10.1140/epjst/e2019-800209-3.
[57] P. Liu, X. Wang, and Y. Su, "Image encryption via complementary embedding algorithm and new spatiotemporal chaotic system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 5, pp. 2506–2519, May 2023, doi: 10.1109/TCSVT.2022.3222559.
[58] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020, doi: 10.1109/ACCESS.2020.2979827.

TA-CHIEN YEH was born in Chang-Hua, Taiwan, in January 1993. He received the B.S. degree in electrical engineering and the M.S. degree in communication engineering from National Taiwan University, Taipei, Taiwan, in 2016 and 2022, respectively. His research interests include signal processing and system simulations.

JEAN-FU KIANG (Life Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1989. Since 1999, he has been a Professor with the Department of Electrical Engineering and the Graduate Institute of Communication Engineering, National Taiwan University, Taipei, Taiwan. His research interests include explore different ideas, theories, and methods on various electromagnetic phenomena and possible applications, including remote sensing, radar signal processing, antennas, phased arrays, propagation, scattering, and communications. Some of his works can be viewed on his website (http://cc.ee.ntu.edu.tw/~jfkiang/selected_publications.html).