The Visual Computer (2021) 37:541–551
https://doi.org/10.1007/s00371-020-01822-8

ORIGINAL ARTICLE

A new one-dimensional cosine polynomial chaotic map and its use in image encryption

Mohamed Zakariya Talhaoui[1] · Xingyuan Wang[1,2] · Mohamed Amine Midoun[1]

Published online: 12 March 2020

Abstract

In this paper, we propose a new real one-dimensional cosine polynomial (1-DCP) chaotic map. The statistical analysis of the proposed map shows that it has a simple structure, a high chaotic behavior, and an infinite chaotic range. Therefore, the proposed map is a perfect candidate for the design of chaos-based cryptographic systems. Moreover, we propose an application of the 1-DCP map in the design of a new efficient image encryption scheme (1-DCPIE) to demonstrate the new map further good cryptographic proprieties. In the new scheme, we significantly reduce the encryption process time by raising the small processing unit from the pixels level to the rows/columns level and replacing the classical sequential permutation substitution architecture with a parallel permutation substitution one. We apply several simulation and security tests on the proposed scheme and compare its performances with some recently proposed encryption schemes. The simulation results prove that 1-DCPIE has a better security level and a higher encryption speed.

Keywords Image encryption · One-dimensional chaotic map · Chaos theory · Secure real-time communication · Cryptography

1 Introduction

Nowadays, the number of digital images is exponentially growing due to the fast development of information technologies. As a consequence, a large number of images are stored and transmitted every second, where a significant part of these images is considered as private content [56]. To guarantee privacy and security, many researchers and security experts developed several types of algorithms, such as steganography [40,53,58], watermarking [3,5,10,29,34], data hiding [9,28,52], and image encryption [19,21,30,38]. Unlike the former types, which tend to hide the secret information into a public image, the image encryption transforms the whole private image into an unrecognized random-like one. Recently, many image encryption schemes have been proposed using various theories and technologies like chaotic maps [19,25,31,41,55], DNA encoding [7,12], quantum theory [13,27], optical systems [24,46,54], etc [14,44]. Among these technologies, chaotic maps are the most popular due to the natural chaos proprieties such as unpredictability, ergodicity, high sensitivity, and a random-like and deterministic behavior. These features perfectly respond to cryptography systems' needs.

In chaos theory, depending on the number of variables, chaotic maps are divided into two categories: low-dimensional and high-dimensional chaotic maps. Low-dimensional chaotic maps have a simple structure and are more easy to implement. However, most of the low-dimensional maps are proved to be predictable due to their small chaotic range [8,22,51]. In contrast, high-dimensional chaotic maps have a more extensive chaotic range but are more complex and consequently more difficult to implement. Discovering some new sources of chaos with better randomness, higher unpredictability, larger chaotic range, and simple structure becomes the main focus of many security researchers [16,17,42,43]. Borgia et al. [2] presented a new one-dimensional chaotic map using a combination of sin and arcsin functions and then apply the proposed map in the design of a real-time image encryption algorithm.

✉ Xingyuan Wang
wangxy@dlut.edu.cn

Mohamed Zakariya Talhaoui
talhaouizakariya@mail.dlut.edu.cn

Mohamed Amine Midoun
aminemidoun31@mail.dlut.edu.cn

[1] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China

[2] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

The proposed encryption scheme has a fast speed,yet the used map is topologically conjugated with the logistic map, which has been proved to be easily predictible [23,39]. In [15], the authors generated a new two-dimensional chaotic map by adjusting the logistic map using the sine map (2D-LASM) and then use the generated map to implement a new encryption system. Unfortunately, the proposed scheme was cryptanlyzed by Feng et al. [11]. In [45], Wang et al. proposed a new color image encryption scheme using a globally customized coupled map lattice. Although the system has a good security level, its encryption speed is too slow.

Motivated by these issues, we propose a new one-dimensional cosine polynomial 1-DCP chaotic map. This new map has a simple mathematical definition and exhibits a high chaotic behavior over an infinite range of its real control parameter values which makes it a perfect candidate for the design of image encryption schemes thanks to its simple structure, high chaotic behavior, and infinite chaotic range. We apply several chaos theory tests to demonstrate the good chaotic performances of the 1-DCP map. Besides, we design a novel efficient image encryption 1-DCPIE scheme based on the proposed map. In 1-DCPIE scheme, we raise the small encryption unit from the pixels level to the rows/columns level which highly increases the encryption speed. Furthermore, we adopt an alternative to the substitution permutation network architecture, where the permutation and substitution phases are merged. This new architecture makes the 1-DCPIE scheme able to withstand separate attacks [47] when only one encryption round is applied and enhances its security and speed. We perform several simulation tests, such as histogram, information entropy, secret key analysis, image sensitivity, and correlation analyses, to prove the high performances of 1-DCPIE.

The rest of the paper is organized as follows. Section 2 presents the 1-DCP chaotic map and evaluates its chaotic behavior. Section 3 describes in detail the proposed 1-DCPIE scheme. In Sect. 4, we simulate the 1-DCPIE scheme and evaluate its performances. Finally, Sect. 5 concludes the paper.

2 The proposed chaotic map

Here, we introduce a new one-dimensional cosine polynomial chaotic system (1-DCP) defined by the following equation (Eq. 1):

$$\begin{cases} f : [-1; 1] \longrightarrow [-1; 1] \\ \quad x_{n+1} = f(x_n) = \cos(\mu(x_n^3 + x_n)) \end{cases} \tag{1}$$

where μ is a real control parameter. Since the new map is bounded by the even function cosine, the sign of μ is not significant. Hence we ignore the negative values of μ. The 1-DCP map exhibits an extremely high chaotic behavior for most of μ values. That makes its chaotic region as large as the infinite space of positive real numbers. Therefore, the 1-DCP map fits more the needs of cryptography in terms of large keyspace, complexity, and unpredictability. In the following section, we analyze the performances of the new map through several dynamical systems tests.

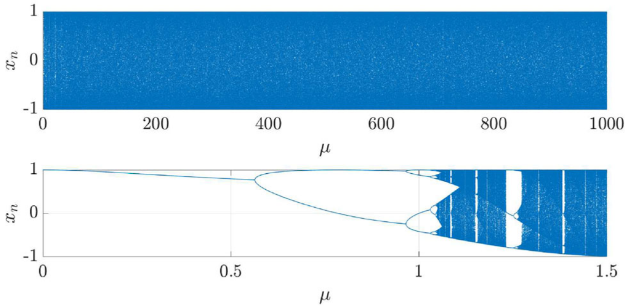


Fig. 1 Bifurcation diagram of 1-DCP using different scales

2.1 Bifurcation and trajectory analysis

The long-term behavior of a dynamical system (stability, instability, periodicity, or chaos) is visually described through the bifurcation diagram as a function of the parameter values. Figure 1 shows the bifurcation diagram of 1-DCP using different scales. The map first settles into one fixed point when $0 \leq \mu < 0.56$, and then it enters into a period-doubling phase for $0.56 \leq \mu < 1.05$, and finally gets into the chaos beyond the point $\mu^* = 1.05$. A few numbers of periodic windows exist in the bifurcation diagram. Figure 2 projects the trajectory of 1-DCP in 2D and 3D phase space. It is seen from the phase diagram that the new map trajectory has a sinusoidal waveform where its periodicity tends to get smaller as the parameter μ gets bigger. As a consequence, the trajectory of 1-DCP looks random-like for the high values of μ.

2.2 Approximate entropy

The approximate entropy (ApEn) [32,33] is a statistical test to calculate the complexity and irregularity of dynamical systems. A positive value of the ApEn test reflects the absence of repetitive patterns among the generated orbits. A higher ApEn value means more complexity and unpredictability of the system. As shown in Fig. 3, the ApEn value of 1-DCP map is positive for $\mu \in [0, 1000]$. Therefore, the generated time series by the new map present no repetitive patterns.Compared to other well-known chaotic maps, the 1-DCP ApEn values are mostly better than the Circle map ApEn values and are comparable to those obtained by the Chebychev map.

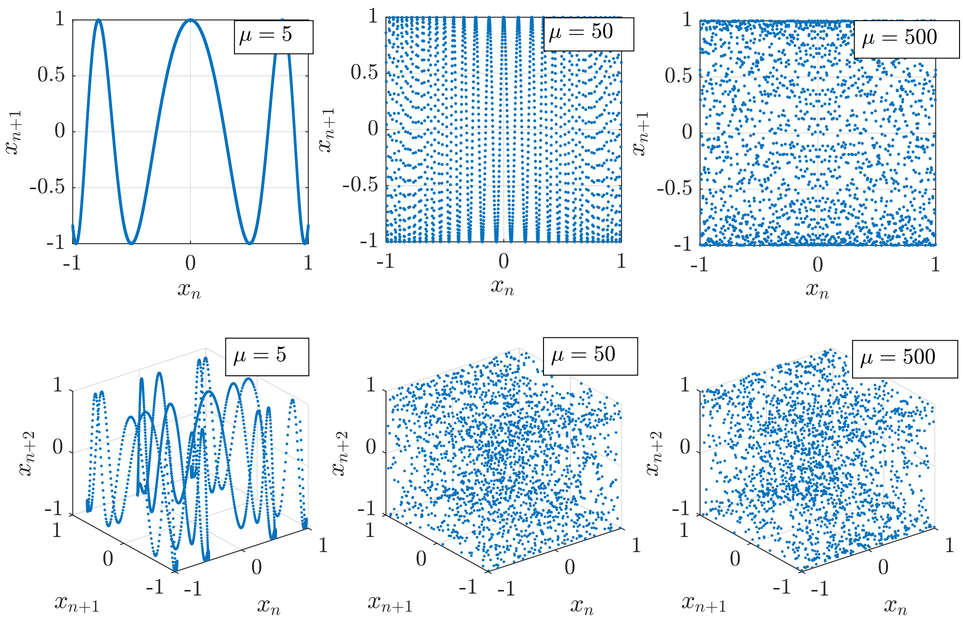


Fig. 2 Phase diagram of 1-DCP using different values of μ

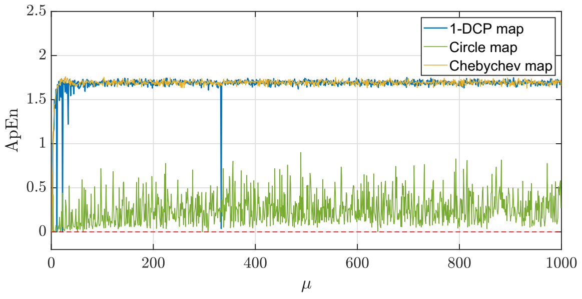


Fig. 3 Approximate entropy analysis and comparison

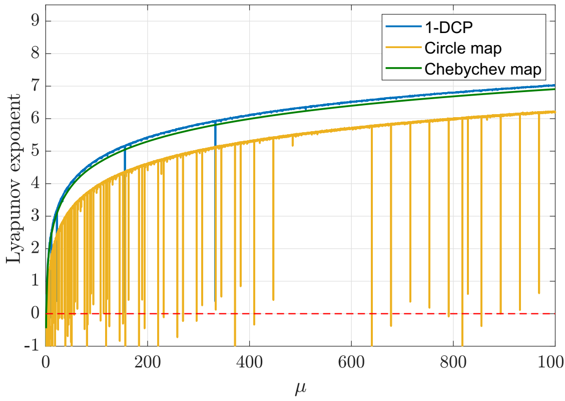


Fig. 4 Lyapunov exponent analysis and comparison

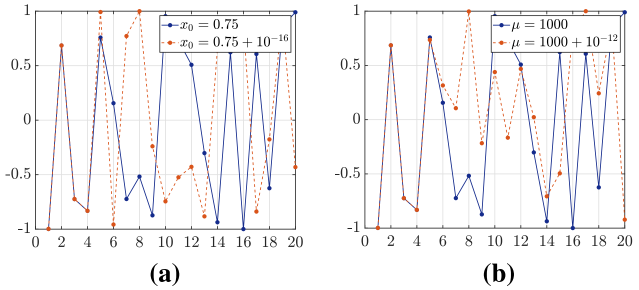


Fig. 5 Sensitivity of 1-DCP to tiny changes At: **a** initial value x_0; **b** parameter value μ

2.3 Initial state sensitivity

The sensitivity to the initial values, which is one of the most important characteristics of chaotic systems, is expressed when orbits with infinitesimally close initial values exponentially diverge after a finite number of iterations. The rate of divergence is usually quantified using the Lyapunov exponent(LE) [Eq. (2)] where a positive LE reflects the system's sensitivity to the initial state and can be comprehended as the existence of a chaotic behavior if the system is bounded. In Fig. 4, we calculate the LE of 1-DCP using Wolf et al. [49] algorithm and plot it against the parameter μ. As shown in Fig. 4, the 1-DCP map has a large positive LE value for most of μ values. In Comparison with some other chaotic maps, the LE of the proposed map is quite better than the LE of the Chebychev and Circle chaotic maps. Besides, to further analyze the sensitivity of the proposed map, we plot two orbits with a 10^{-16} difference between their initial values in Fig. 5a and two orbits with a 10^{-12} difference between their parameter values in Fig. 5b. As shown in these plots, the orbits diverge after only five or six iterations due to the map's high chaotic behavior.

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \ln \mid f'(x_n) \mid \qquad (2)$$

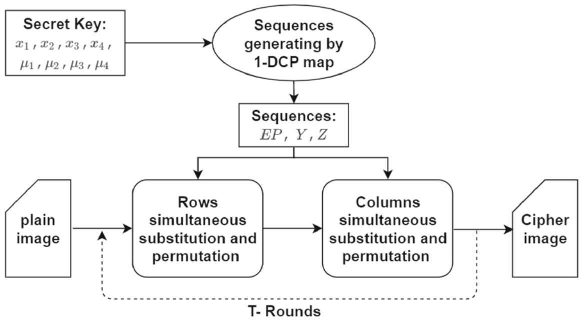

Secret Key:
$x_1, x_2, x_3, x_4,$
$\mu_1, \mu_2, \mu_3, \mu_4$
Sequences generating by 1-DCP map
Sequences:
EP, Y, Z
plain image
Rows simultaneous substitution and permutation
Columns simultaneous substitution and permutation
Cipher image
T- Rounds

Fig. 6 Flowchart of the proposed image encryption scheme 1-DCPIE

3 Image encryption scheme

Here, we propose a new fast image encryption scheme 1-DCPIE based on the 1-DCP chaotic map. Unlike most of the existing encryption schemes, we combine the permutation and the substitution stages to significantly increase the encryption speed by reducing the number of loops over the pixels. Besides, the combination of these two phases makes the new scheme able to withstand the separate attacks. Assuming a plain image P, the encryption process is divided into two modules: a row phase followed by a column phase. To encrypt the image rows, we iterate over the image rows P_i starting from the first to the last row wherein each iteration we encrypt the row P_i and another row $P_{\mathrm{EP}(i)}$ indicated by a key stream EP. Indeed, we mask these two rows values using the predecessor row, a pseudo-random numbers sequences generated from the 1-DCP chaotic map, and the modulo operation. Then, we scramble the row P_i pixels using the circular shifting operation. Finally, we encrypt the columns by transposing the obtained image and reapplying the rows encryption phase. Figure 6 shows the encryption flowchart.

The encryption steps

The detailed encryption steps of the proposed scheme are described as follows

(1) Read the plain image P, round keys x_{ir}, μ_{ir} where $i \in \{1, 2, 3, 4\}, r \in \{1, 2, \ldots, T\}$, and T is the total number of encryption rounds.
(2) Set the round counter $r = 1$.
(3) Set M as the total number of rows and N as the total number of columns.
(4) Use the 1-DCP map to generate encryption positions sequence EP of length M using x_{1r} and μ_{1r} as initial conditions and then apply Eq. 3 to normalize EP values.

$$\mathrm{EP} = \{\mathrm{EP}_i | \mathrm{EP}_i = (\mathrm{EP}_i \times 10^7) \bmod M\} \tag{3}$$

(5) Calculate x_{5r} using the following equation:

$$x_{5r} = x_{1r} + \mathrm{mean}(P/\{P_1, P_{\mathrm{EP}(1)}\})$$

where $\mathrm{mean}(P/\{P_1, P_{\mathrm{EP}(1)}\})$ is the average pixels value of the image P excluding the first and the EP(1) row.

(6) Generate sequences Y, Z of length N with the 1-DCP map using x_{3r}, x_{5r} and μ_{3r}, respectively, as initial conditions. Then, apply Eqs. 4 and 5 to normalize the generated sequences.

$$Y = \{Y_j | Y_j = (Y_j \times 10^7) \bmod 256\} \tag{4}$$
$$Z = \{Z_j | Z_j = (Z_j \times 10^7) \bmod 256\} \tag{5}$$

(7) Starting from the first to the last row, encrypt in each iteration two rows P_i and $P_{\mathrm{EP}(i)}$ as follows.

$$\begin{cases} P_i = \mathrm{circshift}((P_i + f(i) + \mathrm{pred}(i)) \bmod 256, \mathrm{EP}(i)) \\ P_{\mathrm{EP}(i)} = (P_{\mathrm{EP}(i)} + f(i) + \mathrm{pred}(i)) \bmod 256 \end{cases}$$

The $\mathrm{circshift}(P_i, n)$ function is a circular shifting operation of the row P_i to the right n times, and the $f(i)$, $\mathrm{pred}(i)$ functions are defined as follows

$$f(i) = \begin{cases} Y & \text{if } i \neq 1 \\ Z & \text{if } i = 1 \end{cases} \quad \mathrm{pred}(i) = \begin{cases} P_M & \text{if } i = 1 \\ P_{i-1} & \text{else} \end{cases}$$

(8) Transpose the obtained image matrix $P = P^t$ to encrypt the columns and then repeat steps 3–7 using $x_{2r} + \mathrm{mean}(\{X_{ir}\})$, x_{4r}, μ_{2r}, μ_{4r} instead of x_{1r}, x_{3r}, μ_{1r}, μ_{3r} where $i \in \{1, 2, 3, 4\}$ and $\mathrm{mean}(\{X_{ir}\})$ is the average of round key parts.
(9) Transpose back the cipher image $P = P^t$.
(10) Increment the rounds counter $r = r + 1$ and repeat steps 3–9 until $r > T$.

The decryption steps

The decryption of cipher images is easily achieved by inverting the encryption steps as follows.

(1) Read the cipher image P, round keys x_{ir}, μ_{ir} where $i \in \{1, 2, 3, 4\}$, $r \in \{1, 2, \ldots, T\}$, and T is the total number of encryption rounds.
(2) Set the round counter $r = T$.
(3) Transpose the cipher image matrix $P = P^t$ to decrypt the columns.
(4) Set M as the total number of rows and N as the total number of columns.
(5) Use the 1-DCP map to generate encryption positions sequence EP of length M by setting $x_{2r} + \mathrm{mean}(X_r)$

and μ_{2r} as initial conditions and then apply Eq. 3 to normalize EP values.

(6) Generate sequence Y of length N with the 1-DCP map using x_{4r} and μ_{4r}, respectively, as initial conditions. Then, apply Eq. 4 to normalize the obtained sequence.

(7) Starting from the last to the second row, decrypt in each iteration two rows P_i and $P_{\text{EP}(i)}$ as follows.

$$\begin{cases} P_i = (\text{circshift}(P_i, \text{EP}(i)) - Y - \text{pred}(i)) \bmod 256 \\ P_{\text{EP}(i)} = (P_{\text{EP}(i)} - Y - \text{pred}(i)) \bmod 256 \end{cases}$$

(8) Calculate x_{5r} using the following equation:

$$x_{5r} = x_{1r} + \text{mean}(P/\{P_1, P_{\text{EP}(1)}\})$$

(9) Generate sequence Z of length N with the 1-DCP map using x_{5r} and μ_{4r}, respectively, as initial conditions. Then, apply Eq. 5 to normalize the obtained sequence.

(10) decrypt the first row P_1 and the row $P_{\text{EP}(1)}$ using the following equation:

$$\begin{cases} P_1 = (\text{circshift}(C_1, \text{EP}(1)) - Z - P_M) \bmod 256 \\ P_{\text{EP}(1)} = (C_{\text{EP}(1)} - Z - P_M) \bmod 256 \end{cases}$$

(11) Transpose the obtained image matrix $P = P^t$ to decrypt the rows and then repeat steps 4–10 using $x_{1r}, x_{3r}, \mu_{1r}, \mu_{3r}$ instead of $x_{2r} + \text{mean}(\{X_{ir}\})$, $x_{4r}, \mu_{2r}, \mu_{4r}$.

(12) Decrement the encryption rounds counter $r = r - 1$ and repeat steps 3–11 until $r < 1$.

4 Experimentation and security analysis

In this section, we perform a set of image encryption security tests to analyze the security and performances of the 1-DCPIE scheme. The experimentation environment is powered by an Intel I7-7700HQ processor, 16 GB RAM and MATLAB 2018. Besides, we choose the simulation plain images from the well-known 'Miscellaneous' USC-SIPI dataset.

4.1 Histogram analysis

In the statistical attacks, an illegitimate person can hack the scheme by discovering any eventual relation between plain and cipher images pixels' intensity level. Therefore, the encryption scheme must produce cipher images with a uniform equal distribution. Figure 7 shows the pixels intensity levels histogram of plain/cipher images of grayscale and color '*Lena*' image. We can notice that the histogram of the cipher images is flat and equally distributed. Hence, it does not leak any useful information to the attacker. Besides, we use the Chi-square test to prove the cipher image' histogram uniformity further. The Chi-square is calculated as follows.

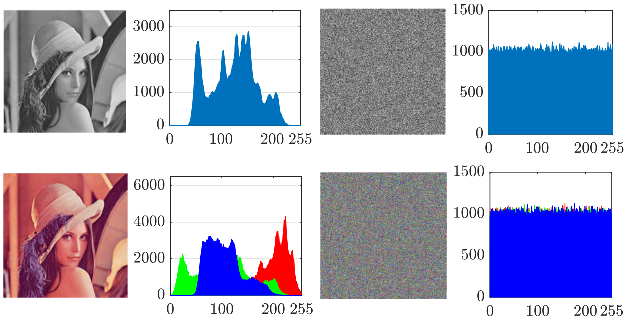


Fig. 7 Grayscale intensity histograms of plain and cipher '*Lena*' images

$$\chi^2 = \sum_{i=0}^{255} \frac{(O_i - E_i)^2}{E_i}$$

where i is the gray-level intensity, O_i is the observed occurrence frequency of the gray level i, and E_i is the expected occurrence frequency of the gray level i. Assuming a significance level $\alpha = 0.05$, the critical value for 8-bit grayscale image is equal to $\chi^2(255, 0.05) = 293.2478$. The Chi-square test value of the generated cipher image by 1-DCPIE is equal to 218.5039 which is lower than the critical value and hence implies that the generated cipher image has a uniform distribution.

4.2 Information entropy analysis

The Shannon entropy [35] can quantify the information uncertainty in a given message m. In image encryption, we apply Shannon entropy to measure information randomness in the produced cipher image C. The theoretical ideal value of information entropy is equal to 8, and the closest is the resulted entropy to the ideal value, the better is the scheme security. The information entropy is calculated as follows

$$H(C) = -\sum_{i=0}^{255} p(C_i) \log_2 p(C_i)$$

where $p(C_i)$ is the occurrence frequency of the pixel value intensity i in the image C. We apply the entropy test 1000 times using random secret keys to encrypt '*Lena*' image by the 1-DCPIE and some recent state of the art schemes, and then we report the results in Table 1. The results show that the new scheme produce cipher images with high entropy using only one encryption round.

In a recent study, Wu et al. [50] proposed the local Shannon entropy (LSE) , which is a new information randomness test more strict and more suitable for image encryption. Unlike

Table 1 Entropy test comparison

	Min	Mean	Std	Max
1-DCPIE (1 round)	7.9991	7.9993	0.000062	7.9996
Ref. [37] (1 round)	7.9976	7.9980	0.000122	7.9984
Ref. [26] (2 round)	7.9991	7.9993	0.000063	7.9995
Ref. [18] (4 round)	7.9980	7.9993	0.000074	7.9995
Ref. [43] (2 round)	7.9991	7.9993	0.000061	7.9995

traditional Shannon entropy, the LSE test measures the average entropy value of k non-overlapping random local blocks. The LSE is calculated as follows

$$\overline{H_{k,T_B}}(C) = \sum_{i=1}^{k} \frac{H(C_i)}{k}$$

where $C_i, i \in \{1, 2, \ldots, k\}$ are k randomly selected blocks, T_B is the block size, and the function $H(C_i)$ calculates the entropy of block C_i. According to the authors, the accepted interval of the LSE test for 8-bit grayscale images is [7.901901; 7.903037]. Table 2 shows the results of the LSE test of the 1-DCPIE and some other schemes applied to the USC-SIPI image database. As one can see, the new scheme achieves an acceptable LSE score in most of the dataset images.

4.3 Plain image sensitivity

The chosen plain text attacks (CPA) are very common and effective attacks against encryption schemes having low sensitivity to the plain image [6,48,57]. Hence, a secure image encryption scheme should always have an avalanche effect for minor changes in the plain images. To test the plain image sensitivity, we use the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) measures. These tests quantitatively evaluate the difference

Table 2 Local Shannon entropy test results

Image name	Ref. [37] (1 round)	Ref. [26] (2 rounds)	Ref. [18] (4 rounds)	Ref. [43] (2 rounds)	1-DCPIE (1 round)
5.1.9	7.899176	7.900580	7.903561	**7.902670**	7.900877
5.1.10	**7.902988**	**7.902470**	7.903468	**7.902930**	**7.902561**
5.1.11	7.900314	7.901817	**7.901932**	7.900260	**7.902094**
5.1.12	**7.902894**	**7.902437**	7.903253	7.901841	**7.902069**
5.1.13	7.899601	**7.902051**	**7.902108**	**7.902954**	7.901226
5.1.14	**7.902881**	7.900493	7.901315	**7.902243**	**7.902006**
5.2.08	7.876082	**7.902264**	**7.902890**	**7.902576**	**7.902629**
5.2.09	7.865113	7.903199	7.901146	7.903387	**7.902055**
5.2.10	7.887348	**7.902912**	**7.902251**	**7.902899**	**7.902886**
5.3.01	7.894821	7.901544	7.901716	**7.902310**	7.903266
5.3.02	7.871267	**7.902522**	7.900810	**7.902043**	**7.902620**
7.1.01	7.857684	7.903668	**7.902888**	**7.902522**	7.905016
7.1.02	7.820918	**7.902807**	7.893779	7.901637	**7.902879**
7.1.03	7.845253	**7.902931**	**7.902349**	**7.902441**	7.901359
7.1.04	7.860630	**7.902478**	**7.902560**	7.901043	**7.901906**
7.1.05	7.874394	7.9058365	**7.902604**	7.905103	**7.901969**
7.1.06	7.870690	**7.902099**	**7.902744**	**7.902917**	**7.902519**
7.1.07	7.849089	**7.902971**	7.909817	7.901422	7.903090
7.1.08	7.837632	**7.902930**	**7.901911**	**7.902774**	**7.902433**
7.1.09	7.866492	7.901604	**7.902666**	**7.902589**	**7.902402**
7.1.10	7.855740	7.900875	**7.902547**	7.903738	**7.902364**
7.2.01	7.818208	**7.902100**	**7.902280**	7.901167	7.904283
Boat.512	7.876833	**7.902474**	**7.901965**	7.901181	**7.901929**
Gray21.512	**7.902961**	7.901099	7.906956	**7.902815**	7.904195
Ruler.512	7.788990	7.904014	7.904462	7.901054	**7.902020**
Pass/All	4/25	14/25	14/25	14/25	**17/25**
Std	0.030400	0.001136	0.001345	0.001016	**0.000940**
Mean	7.869100	7.902407	7.902559	7.902340	**7.902506**

The values written in bold are in the accepted interval of LSE test between the cipher images C and C' generated from two identical plain images having only a slight difference. The NPCR and UACI are defined as follows

$$\mathrm{NPCR}(C, C') = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D_{ij}}{M \times N}$$

$$\mathrm{UACI}(C, C') = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |C_{ij} - C'_{ij}|}{N \times M \times F}$$

where $D_{ij} = 0$ if $C_{ij} = C'_{ij}$ and $D_{ij} = 1$ if $C_{ij} \neq C'_{ij}$ and F is the biggest possible pixel value. According to Wu et al. [4], the NPCR and UACI values with regard to a significance level α must be greater than N_α^* for the NPCR and should belong to $[U_\alpha^{*-}, U_\alpha^{*+}]$ for the UACI. The NPCR/UACI thresholds values are calculated as follows

$$N_\alpha^* = \frac{F - \phi^{-1}(\alpha)}{F + 1} \times \sqrt{\frac{F}{M \times N}}$$

$$\begin{cases} U_\alpha^{*-} = \mu_u + \phi^{-1}(\frac{\alpha}{2}) \times \sigma_u \\ U_\alpha^{*+} = \mu_u - \phi^{-1}(\frac{\alpha}{2}) \times \sigma_u \end{cases}$$

where

$$\mu_u = \frac{F + 2}{3F + 3}, \quad \sigma_u^2 = \frac{(F + 2)(F^2 + 2F + 3)}{18(F + 1)^2 \times F \times M \times N}$$

and $\phi^{-1}(.)$ is the inverse cumulative density function. Table 3 contains the NPCR/UACI thresholds for different image sizes where the significance level is set to $\alpha = 0.05$. We apply the NPCR and UACI tests on the 1-DCPIE scheme, where we slightly modify one random pixel. Figures 8 and 9 show the NPCR/UACI scores obtained by the proposed scheme and some other encryption methods. Figures 10 and 11 show the NPCR and UACI values evolution as a function of the encryption round number r. Besides, since the proposed scheme uses the average function, we reapply the NPCR and UACI tests on '*Lena*' image by adding one to a random pixel and subtracting one from another to get the same average value. The results are reported in Table 4. In comparison, we can notice that the proposed scheme has quite similar results as the other methods. However, the minimum number of encryption rounds is remarkably fewer.

Table 3 Expected NPCR and UACI values

Image size	NPCR N_α^* (%)	UACI U_α^{*-} (%)	UACI U_α^{*+} (%)
256 × 256	99.5693	33.2824	33.6447
512 × 512	99.5893	33.3730	33.5541
1024 × 1024	99.5994	33.4183	33.5088

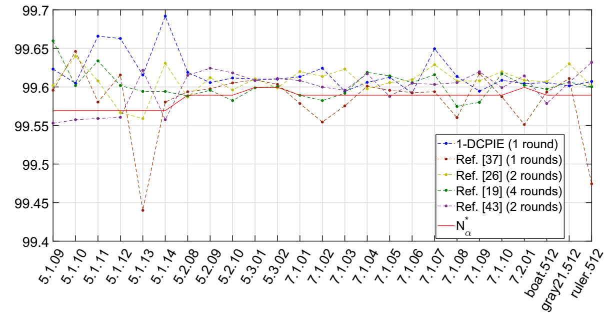


Fig. 8 NPCR test results and comparison

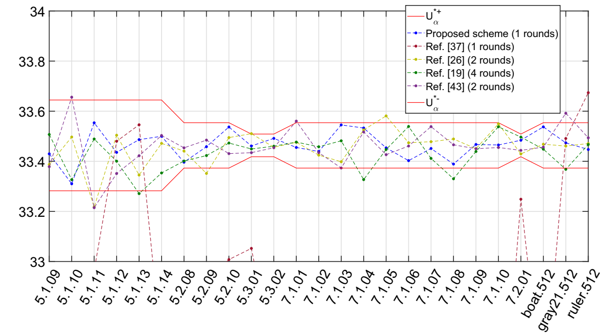


Fig. 9 UACI test results and comparison

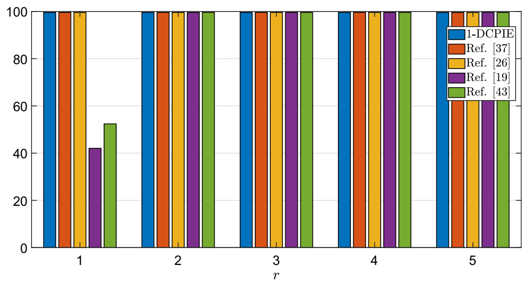


Fig. 10 NPCR evolution over encryption rounds number

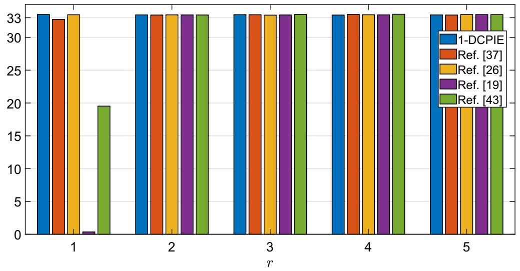


Fig. 11 UACI evolution over encryption rounds number

4.4 Secret key analysis

In cryptography, the keyspace should be as large as possible to resist brute-force attacks where an illegitimate person can decrypt a cipher image by trying all the possible keys. In the 1-DCPIE scheme, we set the combination $\{x_{ir}, \mu_{ir}\}$

Table 4 NPCR/UACI values when changing two pixels

	Pixels average	NPCR	UACI
1-DCPIE (1 round)	Used	99.6407%	33.4386%
Ref. [37] (1 rounds)	Used	0.00076%	0.00013%
Ref. [26] (2 rounds)	Used	0.00076%	0.000002%
Ref. [18] (4 rounds)	Not used	99.6067%	33.3741%
Ref. [43] (2 rounds)	Not used	99.6071%	33.4692%

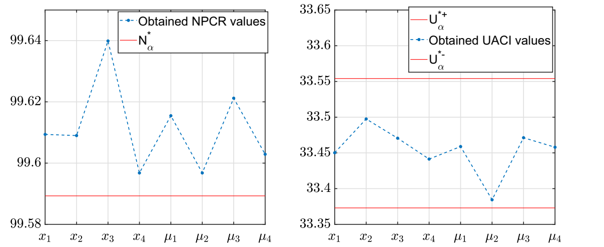


Fig. 12 NPCR and UACI analysis results of 1-DCPIE encryption secret key sensitivity

($i \in \{1, 2, 3, 4\}$, $r \in \{1, 2, \ldots, T\}$ and T is the total number of encryption rounds). In the IEEE-754 standard [20], the precision of the double float type is equal to 10^{-16}. However, the precision of the (1-DCP) control parameter μ is equal to 10^{-12}. Therefore, the 1-DCPIE secret keyspace is approximated as $(10^{16\times 4} \times 10^{12\times 4})^T \approx 2^{392\times T}$, which is largely sufficient to handle brute-force attacks [1,36]. Moreover, the secret key must be sensitive to any minor modification to produce a totally different cipher image whenever it is altered. We apply the NPCR/UACI tests to quantify the difference between the output cipher images encrypted using almost identical secret keys. The obtained results of modifying any part in the key are all in the acceptable range of NPCR/UACI (see Fig. 12). Besides, in Fig. 13 we illustrate the results of key sensitivity in the decryption process where we slightly change a part of the key and try to decrypt the cipher image. We can notice that only the original key can decrypt the cipher image.

4.5 Speed analysis

Nowadays, many image encryption schemes achieve a sufficient security level. However, their encryption algorithms are too complicated, which mainly affect their speed and hence make them inapplicable in real communications. In the new scheme, we aim to increase the processing speed by significantly reducing the chaotic map use, raising the small encryption unit from the pixels level to the rows/columns level, and combining the substitution and permutation stages. In Table 5, we compare the theoretical and experimental speeds of the 1-DCPIE scheme and some recently published encryption schemes which have been simulated in the same running environment.

4.6 Correlation analysis

The adjacent pixels values in the image data type are often close and highly correlated. This image characteristic is a big obstacle for cryptography where an attacker can try to hack the scheme by finding eventual relations between correlation in the plain and cipher images. Therefore, the encryption scheme must break any existing high correlation among adjacent pixels. To test the resistance of the new scheme against this type of attack, we choose 2000 random pixels in both plain and cipher images. Then, we calculate the cor-

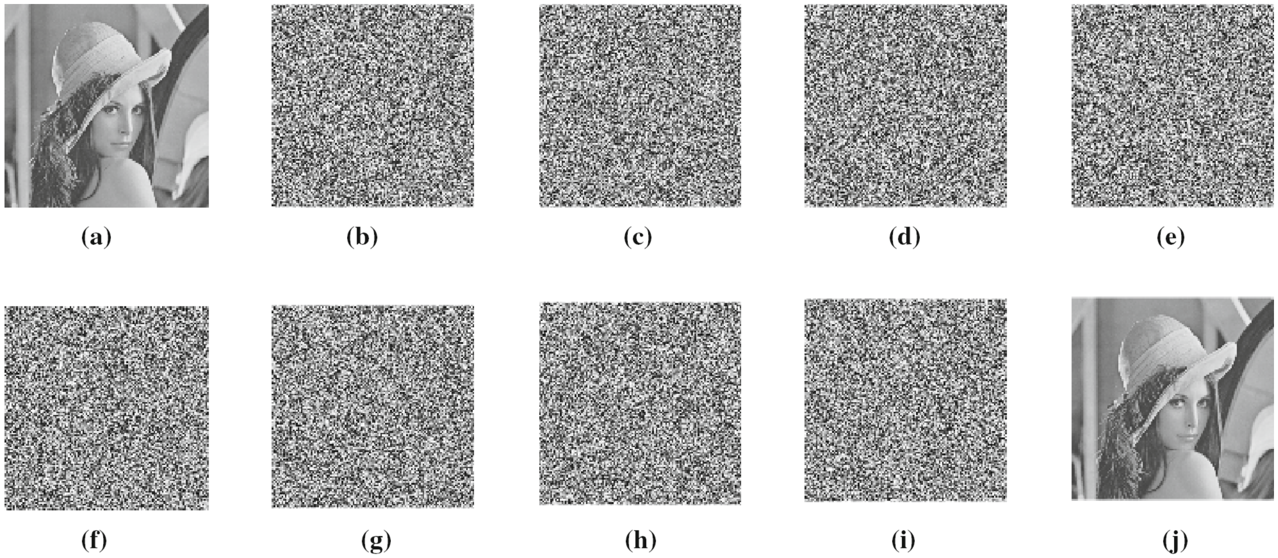


Fig. 13 **a** Plain ‘*Lena*’ image; decryption using slightly modified **b** x_1; **c** x_2; **d** x_3; **e** x_4; **f** μ_1; **g** μ_2; **h** μ_3; **i** μ_4; **j** original key

Table 5 Speed analysis test results (ms)

	Ref. [37]	Ref. [26]	Ref. [18]	Ref. [43]	1-DCPIE
Complexity	$O(MN)$	$O(MN)$	$O(MN)$	$O(MN)$	$O(M+N)$
Minimum rounds	1	2	4	2	1
256 × 256	21.2	75.9	398.8	59.8	11.1
512 × 512	93.9	315.6	1677.4	162.6	36.0
1024 × 1024	387.2	1315.3	6984.1	575.0	134.2

Table 6 Correlation test analysis

	Horizontal	Vertical	Diagonal
Plain image ‘*Lena*’	0.9693	0.9860	0.9572
1-DCPIE	– 0.0076	0.0004	0.0019
Ref. [37]	0.0335	– 0.0174	– 0.0295
Ref. [26]	– 0.0132	0.0185	0.0376
Ref. [18]	0.0097	– 0.0280	0.0247
Ref. [43]	– 0.0059	– 0.0146	0.0211

relation coefficient of the chosen pixels by the following equation:

$$\mathrm{corr}(x, y) = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}}$$

where

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

$$D(x) = \sum_{i=1}^{N}(x_i - E(x))^2, \ E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

The test results are reported in Table 6. The correlation test results prove that the proposed scheme produces cipher images with no correlation.

4.7 Interference resistance analysis

In reality, the transmitted data over communication canals are sometimes altered by the effect of noise interference signals or deliberately by attackers. Thus, some parts of the received cipher images can be lost. An effective encryption scheme must be able to decrypt the rest of the affected cipher image and retrieve the corresponding plain image. Figure 14 illustrates the capacity of 1-DCPIE to decrypt noisy cipher images.

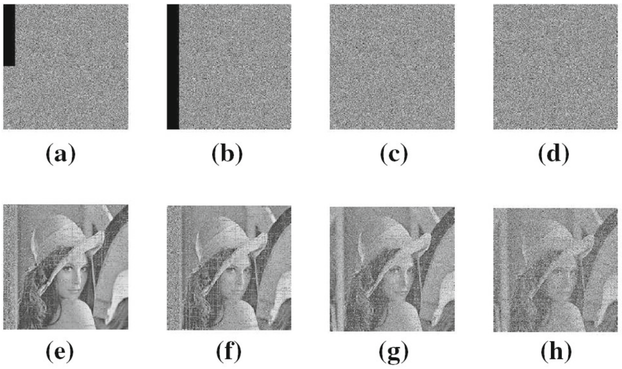


Fig. 14 Interference resistance analysis: **a** cipher image with 5% data loss; **b** cipher image with 10% data loss; **c** cipher image affected by 2.5% of ‘*Salt & Pepper*’ noise; **d** cipher image affected by 5% of ‘*Salt & Pepper*’ noise; **e** decryption of image **a**; **f** decryption of image **b**;**g** decryption of image **c**; **h** decryption of image **d**

5 Conclusion

In this paper, we have developed a new one-dimensional chaotic (1-DCP) map defined by a simple iterative mathematical equation. The new chaotic map exhibits a very high chaotical behavior over a large interval of its positive real control parameter. Therefore, this map fits more the needs of cryptography, such as large keyspace, unpredictability, and speed than some predictable low-dimensional maps or slower high-dimensional maps. Through several analytical tests, we demonstrate the high chaotic behavior of the proposed map. Besides, we design a new efficient image encryption scheme based on the 1-DCP map. In this scheme, we merged the permutation and substitution stages to improve encryption speed and security. The experimental analysis results demonstrate that the 1-DCPIE scheme is more secure and faster than other recently proposed encryption schemes.

Acknowledgements This research is supported by the National Natural Science Foundation of China (No: 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (No: MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105-JH2/103). Jinan City ‘20 uinversities’ funding projects Introducing Innovation Team Program (No:2019GXRC031)

Compliance with ethical standards

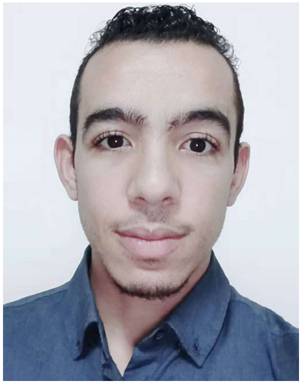
Conflict of interest The authors declare that they have no conflict of interest.

References

1. Alvarez, Li, Shujun, G.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos **16**(08), 2129–2151 (2006)
2. Boriga, R., Dăscălescu, A.C., Diaconu, A.V.: A new one-dimensional chaotic map and its use in a novel real-time image encryption scheme. Adv. Multimed. **2014**, 6 (2014)
3. Cao, L., Men, C., Ji, R.: Nonlinear scrambling-based reversible watermarking for 2d-vector maps. Vis. Comput. **29**(3), 231–237 (2013)
4. Castro, J.C.H., Sierra, J.M., Seznec, A., Izquierdo, A., Ribagorda, A.: The strict avalanche criterion randomness test. Math. Comput. Simul. **68**(1), 1–7 (2005). https://doi.org/10.1016/j.matcom.2004.09.001
5. Chang, H.T., Tsan, C.L.: Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain. Appl. Opt. **44**(29), 6211–9 (2005)
6. Chen, J., Han, F., Qian, W., Yao, Y.D., Zhu, Zl: Cryptanalysis and improvement in an image encryption scheme using combination of the 1d chaotic map. Nonlinear Dyn. **93**(4), 2399–2413 (2018)
7. Chen, J., Zhu, Z.L., Zhang, L.B., Zhang, Y., Yang, B.Q.: Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. Signal Process. **142**, 340–353 (2018)
8. Chen, S., Lü, J.: Parameters identification and synchronization of chaotic systems based upon adaptive control. Phys. Lett. A **299**(4), 353–358 (2002)
9. Ding, H., Zichen, L.I., Yang, Y., You, F., Liu, F.: High quality data hiding in halftone image based on block conjugate. Chin. J. Electron. **27**(1), 150–158 (2018)
10. Ernawan, F., Kabir, M.N.: A block-based RDWT-SVD image watermarking method using human visual system characteristics. Vis Comput **36**, 1–19 (2018)
11. Feng, W., He, Y., Li, H., Li, C.: Cryptanalysis and improvement of the image encryption scheme based on 2d logistic-adjusted-sine map. IEEE Access (2019)
12. Fu, X.Q., Liu, B.C., Xie, Y.Y., Wei, L., Yong, L.: Image encryption-then-transmission using dna encryption algorithm and the double chaos. IEEE Photon. J. **PP**(99), 1–1 (2018)
13. Hu, Y., Xie, X., Liu, X., Zhou, N.: Quantum multi-image encryption based on iteration arnold transform with parameters and image correlation decomposition. Int. J. Theor. Phys. **56**(7), 2192–2205 (2017)
14. Hua, Z., Xu, B., Jin, F., Huang, H.: Image encryption using Josephus problem and filtering diffusion. IEEE Access **7**, 8660–8674 (2019)
15. Hua, Z., Zhou, Y.: Image encryption using 2d logistic-adjusted-Sine map. Inf. Sci. **339**, 237–253 (2016)
16. Hua, Z., Zhou, Y.: Exponential chaotic model for generating robust chaos. In: IEEE transactions on systems, man, and cybernetics: systems (2019)
17. Hua, Z., Zhou, Y., Bao, B. C.: Two-dimensional sine chaotification system with hardware implementation. IEEE Trans. Ind. Inf. (2019)
18. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. **480**, 403–419 (2019)
19. Huang, L., Cai, S., Xiao, M., Xiong, X.: A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion. Entropy **20**(7), 535 (2018)
20. IEEE standard for binary floating-point arithmetic. Institute of Electrical and Electronics Engineers, New York (1985)
21. Kaur, M., Kumar, V.: Fourier-mellin moment-based intertwining map for image encryption. Mod. Phys. Lett. B **32**(9), 1850115 (2018)
22. Kay, S., Nagesha, V.: Methods for chaotic signal estimation. IEEE Trans. Signal Process. **43**(8), 2013–2016 (1995)
23. Li, C., Xie, T., Liu, Q., Cheng, G.: Cryptanalyzing image encryption using chaotic logistic map. Nonlinear Dyn. **78**(2), 1545–1551 (2014)
24. Li, Gd, et al.: Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform. Vis. Comput. **35**(9), 1267–1277 (2019)
25. Liu, H., Kadir, A., Sun, X.: Chaos-based fast colour image encryption scheme with true random number keys from environmental noise. IET Image Process. **11**(5), 324–332 (2017)
26. Liu, L., Miao, S.: A new simple one-dimensional chaotic map and its application for image encryption. Multimed. Tools Appl. **77**(16), 21445–21462 (2018)
27. Liu, X., Xiao, H., Panchi, L.I., Zhao, Y.: Design and implementation of color image encryption based on qubit rotation about axis. Chin. J. Electron. **27**(4), 137–145 (2018)
28. Liu, Z.L., Pun, C.M.: Reversible data-hiding in encrypted images by redundant space transfer. Inf. Sci. **433**, 188–203 (2018)
29. Luong, Q.: A blind image watermarking using multiresolution visibility map. J. Glob. Optim. **49**(3), 435–448 (2011)
30. Muhammad, K., Hamza, R., Ahmad, J., Lloret, J., Wang, H.H.G., Baik, S.W.: Secure surveillance framework for iot systems using probabilistic image encryption. IEEE Trans. Ind. Inf. **PP**(99), 1–1 (2018)
31. Pak, C., Huang, L.: A new color image encryption using combination of the 1d chaotic map. Signal Process. **138**, 129–137 (2017)
32. Pincus, S.: Approximate entropy (apen) as a complexity measure. Chaos Interdiscip. J. Nonlinear Sci. **5**(1), 110–117 (1995)
33. Pincus, S.M.: Approximate entropy as a measure of system complexity. Proc. Natl. Acad. Sci. **88**(6), 2297–2301 (1991)
34. Seo, J.S., Yoo, C.D.: Localized image watermarking based on feature points of scale-space representation. Pattern Recognit. **37**(7), 1365–1375 (2004)
35. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949). https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
36. Stallings, W.: Cryptography and network security: principles and practice. Int. J. Eng. Comput. Sci. **01**(01), 121–136 (2012)
37. Tang, J., Yu, Z., Liu, L.: A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption. In: Multimedia Tools and Applications, pp. 1–24 (2019)
38. Vaidyanathan, S., Akgul, A., Kaçar, S., Çavuşoğlu, U.: A new 4-d chaotic hyperjerk system, its synchronization, circuit design and applications in rng, image encryption and chaos-based steganography. Eur. Phys. J. Plus **133**(2), 46 (2018)
39. Wang, B., Wei, X., Zhang, Q.: Cryptanalysis of an image cryptosystem based on logistic map. Opt. Int. J. Light Electron. Opt. **124**(14), 1773–1776 (2013)
40. Wang, C., Wang, H., Ji, Y.: Multi-bit wavelength coding phase-shift-keying optical steganography based on amplified spontaneous emission noise. Opt. Commun. **407**, 1–8 (2018)
41. Wang, M., Wang, X., Zhang, Y., Gao, Z.: A novel chaotic encryption scheme based on image segmentation and multiple diffusion models. Opt. Laser Technol. **108**, 558–573 (2018)
42. Wang, M., Wang, X., Zhang, Y., Zhou, S., Zhao, T., Yao, N.: A novel chaotic system and its application in a color image cryptosystem. Opt. Lasers Eng. **121**, 479–494 (2019)

43. Wang, X., Feng, L., Li, R., Zhang, F.: A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. Nonlinear Dyn 1–28 (2019)
44. Wang, X., Gao, S.: Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. Inf. Sci. **507**, 16–36 (2020)
45. Wang, X., Qin, X., Liu, C.: Color image encryption algorithm based on customized globally coupled map lattices. Multimed. Tools Appl. **78**(5), 6191–6209 (2019)
46. Wang, X., Zhou, G., Dai, C., Chen, J.: Optical image encryption with divergent illumination and asymmetric keys. IEEE Photon. J. **PP**(99), 1–1 (2017)
47. Wang, Y., Wong, K.W., Liao, X., Xiang, T., Chen, G.: A chaos-based image encryption algorithm with variable control parameters. Chaos Solitons Fract. **41**(4), 1773–1783 (2009)
48. Wen, W., Zhang, Y., Su, M., Zhang, R., Chen, Jx, Li, M.: Differential attack on a hyper-chaos-based image cryptosystem with a classic bi-modular architecture. Nonlinear Dyn. **87**(1), 383–390 (2017)
49. Wolf, A., Swift, J.B., Swinney, H.L., Vastano, J.A.: Determining lyapunov exponents from a time series. Phys. D Nonlinear Phenom. **16**(3), 285–317 (1985)
50. Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J.P., Natarajan, P.: Local Shannon entropy measure with statistical tests for image randomness. Inf. Sci. **222**, 323–342 (2013). https://doi.org/10.1016/j.ins.2012.07.049
51. Xiaofu, W., Songgeng, S.: A general efficient method for chaotic signal estimation. IEEE Trans. Signal Process. **47**(5), 1424–1428 (1999)
52. Xu, J., Mao, X., Jin, X., Jaffer, A., Lu, S., Li, L., Toyoura, M.: Hidden message in a deformation-based texture. Vis. Comput. **31**(12), 1653–1669 (2015)
53. Yang, Z., Guo, X., Chen, Z., Huang, Y., Zhang, Y.J.: RNN-STEGA: linguistic steganography based on recurrent neural networks. IEEE Trans. Inf. Forensics Secur. **PP**(99), 1–1 (2018)
54. Yao, S., Chen, L., Chang, G., He, B.: A new optical encryption system for image transformation. Opt. Laser Technol. **97**, 234–241 (2017)
55. Zhang, X., Wang, X.: Multiple-image encryption algorithm based on mixed image element and chaos. Comput. Electr. Eng. **92**, 6–16 (2017)
56. Zhang, Y., He, Q., Xiang, Y., Zhang, L.Y., Liu, B., Chen, J., Xie, Y.: Low-cost and confidentiality-preserving data acquisition for internet of multimedia things. IEEE Int. Things J. **5**(5), 3442–3451 (2017)
57. Zhang, Y., Li, Y., Wen, W., Wu, Y., Chen, Jx: Deciphering an image cipher based on 3-cell chaotic map and biological operations. Nonlinear Dyn. **82**(4), 1831–1837 (2015)
58. Zhou, R.G., Luo, J., Liu, X.A., Zhu, C., Wei, L., Zhang, X.: A novel quantum image steganography scheme based on LSB. Int. J. Theor. Phys. **57**(1), 1–16 (2018)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Mohamed Zakariya Talhaoui born in 1992, is a Ph.D. student in the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, China. In 2014, he received a bachelors degree in "Information and Communication Science and technology" at the University of ORAN 1 Ahmed Ben-Bella. Then, he obtained a masters degree in "Knowledge and Information of Web Technologies" from the same university in 2016. His current research interests include nonlinear dynamics, image processing, chaos cryptography, and multimedia security.

Xingyuan Wang received the Ph.D. degree in computer software and theory from Northeast University, China, 1999. From 1999 to 2001, he was a postdoctoral researcher at Northeast University. He is currently a professor with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, China. He has published four books and more than 400 scientific papers in refereed journals and proceedings. His research interests include nonlinear dynamics and control, image processing, chaos cryptography, systems biology, and complex networks.

Mohamed Amine Midoun born in 1993, is a Ph.D. student at the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, China. He received a masters degree in "networks and distributed systems" at the University of Science and Technology "Mohamed boudiaf," ORAN. His current research interests include nonlinear dynamics, chaos cryptography, community detection, complex networks, and multimedia security.