



A new fast double-chaotic based Image encryption scheme

Roayat Ismail Abdelfatah¹ 

Received: 6 February 2019 / Revised: 20 July 2019 / Accepted: 13 September 2019 /
Published online: 26 October 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

In this paper, a new scheme for image encryption based on a double chaotic pseudo random generator (DCPG), simple XOR and shift rotations operations is proposed. The DCPG is a combination of both Tent and Chebyshev chaotic and so it needs three values of control parameters which are used as shared secret keys. The encryption consists of two rounds. In the first round, the hash value of the input image is computed using SHA-512. This value also is used as a forth shared secret key and from which, 4 amounts of the shift rotations are extracted. A pseudorandom sequence is generated using the proposed DCPG with the same size of the input image. This sequence and also the input image are divided into blocks of size 1×8 . Each block of input image is processed with the corresponding block of the pseudorandom sequence using simple shift rotation and XOR operation. To extend the effect of the original image one pixel change to all the pixels of the cipher image, a second round of XOR operation is added. The proposed scheme has many advantages. It is highly secure due to two reasons. Firstly, it uses four secret keys for encryption which provides a large key space to overcome all types of brute force attacks. Secondly, the amounts of shift rotation used are input image dependent which achieves a strong resistance against chosen plaintext attacks. Also, it is more efficient compared to other recently existing schemes as it consists only of two rounds of simple operations. Security analysis of scheme has been provided. Based on the results, our scheme is highly secure with a reduced encryption time and so it can be used for many applications which require real time secure image communications.

Keywords Image encryption · Chebyshev chaotic · Tent chaotic · XOR · Rotations

1 Introduction

Nowadays, the wide extension of communication networks makes access to digital images very easy. Therefore, the main concern of researchers in this area is to propose new techniques for making

✉ Roayat Ismail Abdelfatah
roayat_esmaeel@f-eng.tanta.edu.eg; roayatismail2016@gmail.com

¹ Faculty of Engineering, Electronics, and Electrical Communications Department, Tanta University, Tanta, Egypt

the images transmission more secure and preventing the illegal users and attacker from accessing it. Image encryption is used to achieve image security. Several conventional encryption schemes as AES [2] and DES have been introduced. But such schemes are time consuming and take long time for image due to its characteristics as redundancy and correlation between pixels. One solution to minimize the computational time of image encryption with such algorithm and achieve low cost secure system is using selective encryption that selects some parts only of the image to encrypt as in [15, 38, 41]. Many recent chaotic based systems for image encryption are introduced [3, 33, 64]. These systems provide a good security level due to the chaos's properties as the ergodicity, the pseudo randomness and sensitivity to the initial values. The one dimension chaotic map has many advantages due to its simplicity and it can be easily implemented so it used to generate pseudorandom key sequence for real time encryption of large data. But such chaotic has a disadvantage in its security due to the simplicity and small key space. So the improvement of the one dimension chaotic maps security becomes an important research point as proposed in [35, 40, 42, 48]. Chebyshev map has been used in several image encryption schemes as in [31, 54, 61]. Tent map too has been used for image encryption in [12, 21, 36]. Chebyshev's chaotic is iterated as following:

$$z_{n+1} = \cos(k * \cos^{-1}(z_n)) \quad \text{where } z_n \in [-1, 1] \quad (1)$$

Where n is the time index, k is the control parameter and z_0 is the initial value.

While Tent map is a one dimension map given in Eq. (2).

$$z_{n+1} = \mu * (1 - 2 * \text{Abs}[z_n - 0.5]) \quad (2)$$

Where: z_0 is initial value, $z_n \in [0, 1]$, $\mu \in (0, 2)$ is control parameter and.

Abs. is the absolute value.

The contribution of this paper is to introduce a new image encryption scheme which achieves high level of security and efficiency that makes it suitable for real time secure image communications. It is based on simple XOR, shift rotations operations and uses DCPG which combines Chebyshev and Tent maps for generating pseudorandom sequence. The proposed DCPG needs three control parameters which are used as shared secret keys between the sender and receiver. This increases the key space of the proposed scheme and hence its strength against different types of attacks. Also, hash function of the input image; which is used as the forth secret key; is used for generation of the values of shift rotations required by the scheme. This makes the scheme immune against chosen plaintext attack. Hash functions provide message integrity and authentication [46]. The scheme includes only two rounds of simple operations so it is fast compared to other existing schemes. The results and analysis prove that our scheme is highly secure and has low cost.

Our paper is organized as following: related work is presented in Section 2, Section 3 presents our proposed scheme, Section 4 introduces performance analysis and simulation results, Section 5 gives comparison analysis. Finally, Section 6 gives conclusions.

2 Related work

Information security can be achieved using two main tools; cryptography and steganography. These two topics have attracted many researchers recently. Steganography schemes

have been proposed in many publications as in [1, 4, 8, 10, 26–28, 52] while many cryptography schemes have been presented as in [5–7, 9, 11, 19, 20, 23, 25, 39, 51, 53, 62]. Random behavior is one of chaotic system characteristics besides its sensitivity to initial conditions. Chaos differs from cryptography that finite sets define encryption transformations, while chaos has meaning only on real numbers [49]. A block chaotic image encryption scheme based on self-adaptive modelling is presented in [60]. In [50], a chaos-based encryption technique to protect ECG packets for time critical tele cardiology applications is proposed. An image encryption algorithm based on double chaotic maps and SHA-3 is presented in [59]. A two-dimensional Logistic-adjusted-Sine map is proposed in [29] and tried to examine the algorithm against attacks. In [55] an encryption based on 2D Logistic map is proposed and it tries to ensure both confusion and diffusion properties from statistical point of view. Logistic map is introduced in [47] by dividing image into blocks and XOR by chaotic map. A Chebyshev function is used to generate a secret key for encrypt the image and uses 2D Chebyshev to enhance the security in [30]. Rectangular transform with Tent map form a combination for encryption and generation of secret key in [56]. In [44], authors propose 1D-chaotic map to reconstruct the measurement matrix for compress sensing that used for encryption and decryption. A combination of the pixel shuffling and changing the gray values of image pixels is suggested using Baker map to shuffle and logistic map to encrypt in spatial domain [24]. A parallel chaotic hashing model is proposed to generate chaotic hash function [37]. Video encryption method is introduced in [32] where encrypt frames using 4D and 3D Arnolds cat map and generate pseudorandom numbers by using Chebyshev map. Bakers map encrypts image in spatial domain in [13]. Selective encryption scheme scalable video coding is used to perform transparent encryption in [14]. In [34], authors propose interleaved computer-generated holograms encryption. The memristive hyper chaotic system, cellular automata and DNA sequence operations is proposed to encrypt image in [16]. A bit level and chaotic based image encryption was proposed in [58]. In [18], image encryption is achieved with synchronous permutation and diffusion technique. Rotation matrix bit level permutation and block diffusion is used for image in [63]. Authors used confusion and diffusion based on improved Skew Tent map for image encryption in [22]. An image encryption scheme using chaotic and AES is introduced in [57]. The pseudo randomness of a sequence produced by a chaotic map can be tested by using one of the most popular standards for the pseudo-random number test of the binary data, named SP800–22 tests by NIST. NIST includes 17 type of testing [43] which are listed in Table 1. These tests compute one or more P values. The test passes if computed P value is above 0.01, otherwise, the test fails.

3 The proposed scheme

3.1 Double chaotic pseudorandom generator (DCPG)

A single one dimension chaotic maps as Chebyshev or Tent maps is simple but needs only one control parameter and the initial value. In the proposed scheme, a combination of Chebyshev and Tent map will be used as shown in Fig. 1 and Eq. (3):

$$z_{n+1} = \mu * (1 - 2 * (Abs[Cos(k * cos^{-1}(z_n)) - 0.5])) \quad (3)$$

Table 1 SP800–22 tests on the generated 10^6 bit binary sequence with 10^3 iterations of experiments

Test name	<i>P</i> value	Test result
Monobit frequency	0.1136	Passed
Block frequency	0.4061	Passed
Runs	0.3806	Passed
Longest-run-of-ones in a block	0.7524	Passed
Binary matrix rank	0.8055	Passed
Discrete Fourier transform (spectral)	0.3307	Passed
Non-overlapping template matching	0.8548	Passed
Overlapping template matching	0.9951	Passed
Maurer’s universal statistical	0.4181	Passed
Linear complexity	0.1407	Passed
Serial test	{0.9864, 0.6624}	Passed
Approximate entropy	0.9305	Passed
Cumulative sums	0.09952	Passed
Random excursions	{0.6917, 0.5117, 0.9854, 0.6136, 0.2915, 0.7810, 0.6336, 0.0882}	Passed
Random excursion variant	{0.4047, 0.5509, 0.4954, 0.5145, 0.7596, 0.7455, 0.8737, 0.5609, 0.6356, 0.6569, 0.5609, 0.2954, 0.2267, 0.1467, 0.0985, 0.1392, 0.3055, 0.6561}	Passed
Cumulative sums test reverse	0.1431	Passed
LempelZiv compression	0.5826	Passed

Where μ and k are control parameters, z_0 is initial value and $z_n \in [0, 1]$. So combining two chaotic maps increases the number of control parameters to three values. These three values besides the hash value of the input image will be used as secret keys known only to the communicating parties. With this increase of secret values, the key space is increased and also the strength of the scheme against different types of attacks.

The results of testing a binary sequence of length 10^6 bit generated by the proposed Tent-Chebyshev chaotic map by SP800–22 with 10^3 iterations of experiments are given in Table 1 and Fig. 2. As in Table 1, all the computed *P*-values are above 0.01 and the generated sequence pass all SP800–22 tests.

According to Table 1 and Fig. 2, the generated sequence from the proposed DCPG has a good randomness.

3.2 The encryption scheme

The flowchart of the proposed scheme is shown in Fig. 3.

The proposed encryption scheme includes two rounds. Assume a $M \times N$ grayscale image *P*, its pixel falls in the interval [0,255]. To encrypt the image *P*, we do the following:

- Step 1: Compute the hash function *H* for the input image *P* by using SHA-512 which consists of 512 bit. This value will be a secret value known only to the two communicating parties. Convert *H* to decimal digits sequence then pad it with zeros

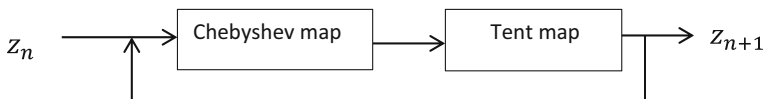


Fig. 1 The proposed DCPG

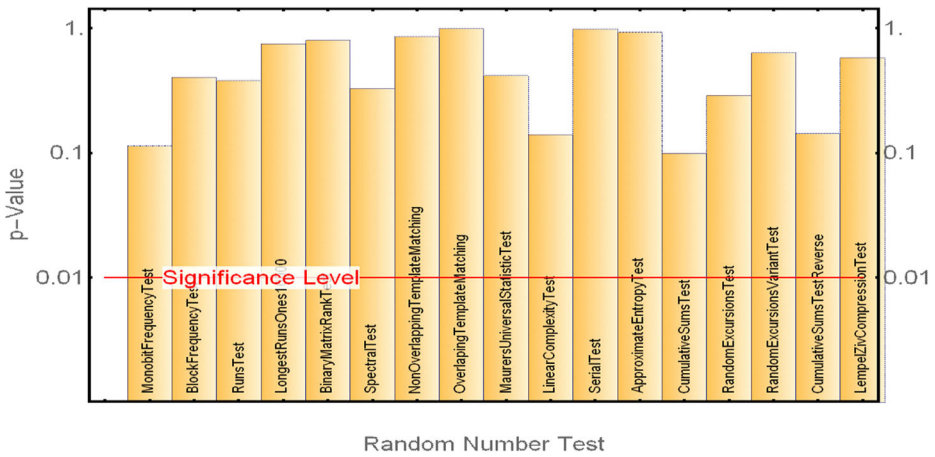


Fig. 2 The results of SP800–22 tests on the generated 10^6 bit binary sequence

to be multiple of 4 then divide the padded sequence into 4 equal length sequences $\{h_1, h_2, \dots, h_4\}$.

Step 2: Compute the 4 values of the shift rotations as following:

$$r_i = h_i \bmod 8, \quad 1 \leq i \leq 4 \tag{4}$$

Step 3: Read the input grayscale image P as a $M \times N$ matrix of pixels. Reshape this matrix into a $1 \times MN$ one, B then divide it into blocks B_i of size 1×8 where;

$$B = \{B_1, B_2, \dots, B_{MN/8}\} \text{ and } B_i = \{b_1, b_2, \dots, b_8\}, \quad 1 \leq i \leq MN/8 \tag{5}$$

Step 4: Select appropriate values for μ, k and z_0 for the proposed DCPG which generates a chaotic sequence $z = \{z_1, z_2, \dots, z_{M \times N}\}$ using Eq. (3) then convert this floating point sequence z into an integer sequence in the range $[0, 255]$, $C = \{C_1, C_2, \dots, C_{M \times N}\}$, using the Eq. (6).

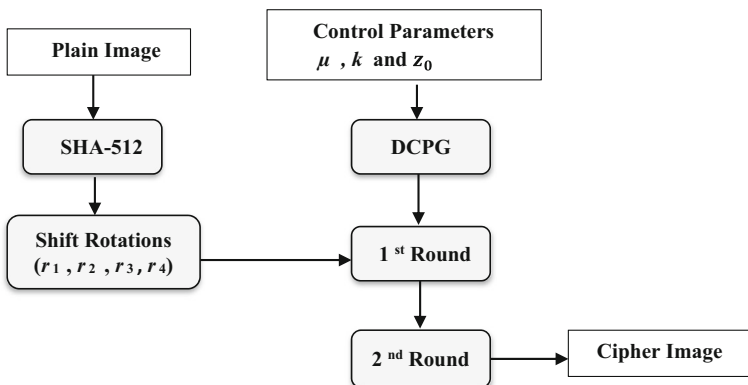


Fig. 3 Encryption Flowchart

$$C_k = \text{floor} (z_k \times 10^{14}) \bmod 256, k = 1, 2, \dots, M \times N \tag{6}$$

Divide C into $MN/8$ blocks K_i , each of size 1×8 , where $K_i = \{k_1, k_2 \dots k_8\}$, $i = 1, 2, \dots, MN/8$ as in Fig. 4.

Step 5: The encryption scheme consists of two rounds.

The 1st round of encryption Figure 5 indicates the first round for each block B_i . In this figure, $b_i' = k_1 \oplus b_{2i} \oplus b_{3i} \oplus b_{4i} \oplus b_{5i} \oplus b_{6i} \oplus b_{7i} \oplus b_{8i}$.

where $b_{1i}, b_{2i}, b_{3i}, b_{4i}, b_{5i}, b_{6i}, b_{7i}, b_{8i}$ are the 8 pixels of each input block B_i and $b_{1o}, b_{2o}, b_{3o}, b_{4o}, b_{5o}, b_{6o}, b_{7o}, b_{8o}$ are the corresponding 8 pixels of each output block B_o .

From Fig. 4, the 8 pixels of the each output block B_o are given by the following equations:

$$b_{2o} = b_{1i} \oplus b_i' \tag{7}$$

$$b_{3o} = \left[(b_{2o})^{<<<r1} \right] \oplus k_2 \oplus b_{2i} \tag{8}$$

$$b_{4o} = b_{3o} \oplus k_3 \oplus b_{3i} \tag{9}$$

$$b_{5o} = \left[(b_{4o})^{<<<r2} \right] \oplus k_4 \oplus b_{4i} \tag{10}$$

$$b_{6o} = b_{5o} \oplus k_5 \oplus b_{5i} \tag{11}$$

$$b_{7o} = \left[(b_{6o})^{<<<r3} \right] \oplus k_6 \oplus b_{6i} \tag{12}$$

$$\begin{aligned} b_{8o} &= b_{7o} \oplus k_7 \oplus b_{7i} \\ b_{1o} &= \left[(b_{8o})^{<<<r4} \right] \oplus k_8 \oplus b_{8i} \end{aligned} \tag{13}$$

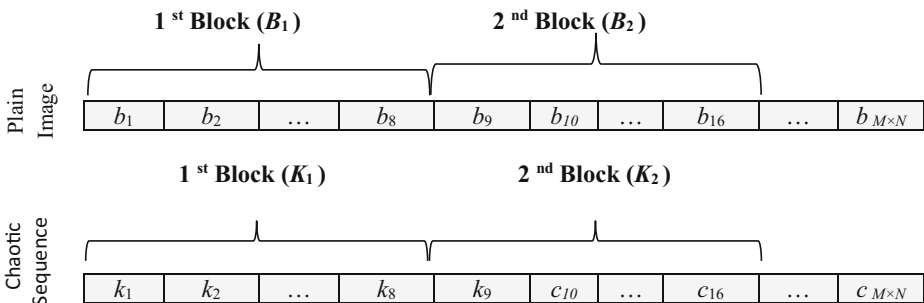


Fig. 4 Image preparation and chaotic sequence generation

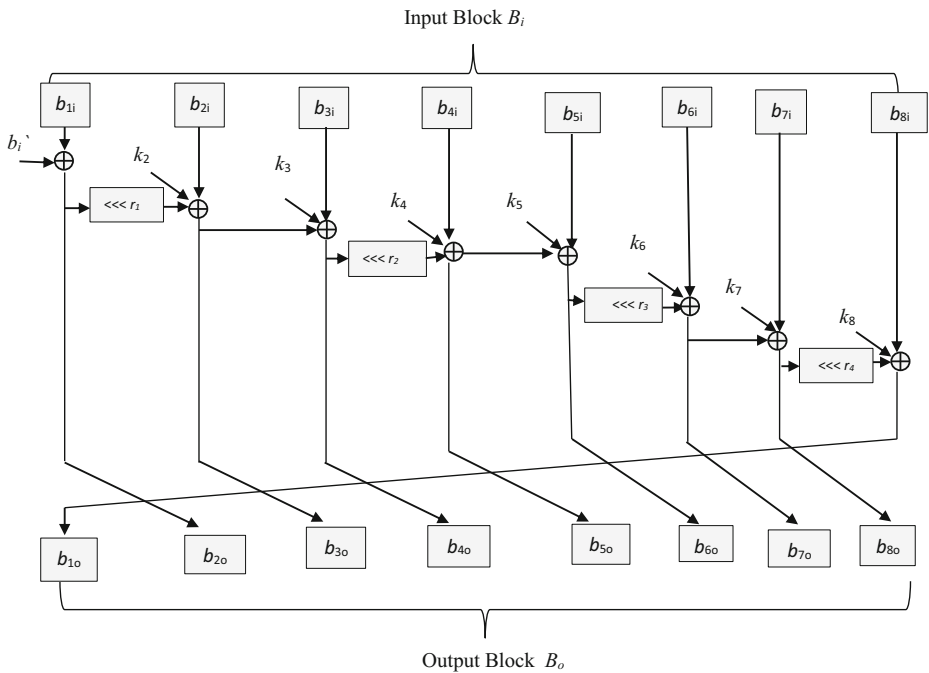


Fig. 5 First round of operation for each input block B_i

According to these equations, if the value of any pixel of the 8 pixels that consist an input block B_i of the original image changed, it affects the 8 pixels of the corresponding output block, B_o of the cipher image. To extend the effect of the original image one pixel change to all the pixels of the cipher image, a second round of operation will be added as following:

The 2nd round of encryption

- Join the output blocks B_o of the first round to form a matrix of size $(1 \times MN)$, then reshape it into another one of size $(\frac{MN}{8} \times 8)$, with number of row = $\frac{MN}{8}$ and number of columns = 8.
- For each row R_i of 8 pixels apply the following function:

$$R_i = R_i \oplus R_{i-1} \quad \text{where } 2 \leq i \leq \frac{MN}{8} \tag{14}$$

- Finally reshape the output matrix into a $M \times N$ matrix to obtain the cipher image C .

3.3 The decryption scheme

By reversing the steps of the encryption scheme, we can recover the input plain image through the decryption as following:

The 1st round of decryption It is as the 2nd round of encryption:

- Read the input grayscale cipher image C as a $M \times N$ matrix of pixels. Reshape it into another one of size $(\frac{MN}{8} \times 8)$, with number of row = $\frac{MN}{8}$ and number of columns = 8.
- For each row RC_i of 8 pixels apply the following function:

$$RC_i = RC_i \oplus RC_{i-1} \quad \text{where } 2 \leq i \leq \frac{MN}{8} \tag{15}$$

The 2nd round of decryption It is as the 1st round of encryption:

1. Reshape the matrix obtained from the 1st round of decryption into a $1 \times MN$ one, Bc then divide it into blocks Bc_i of size 1×8 where

$$Bc = \{Bc_1, Bc_2, \dots, Bc_{MN/8}\} \text{ and } Bc_i = \{bc_1, bc_2, \dots, bc_8\}, 1 \leq i \leq MN/8 \tag{16}$$

2. Use the shared secret values μ, k and z_0 for the proposed DCPG to generates the same chaotic sequence used for encryption $z = \{z_1, z_2, \dots, z_{M \times N}\}$ using Eq. (3) then convert this floating point sequence z into an integer sequence in the range $[0, 255]$, $C = \{C_1, C_2, \dots, C_{M \times N}\}$, using the Eq. (6). Divide C into $MN/8$ blocks K_i , each of size 1×8 , where $K_i = \{k_1, k_2, \dots, k_8\}, i = 1, 2, \dots, MN/8$ as in Fig. 4.
3. $bc_{1i}, bc_{2i}, bc_{3i}, bc_{4i}, bc_{5i}, bc_{6i}, bc_{7i}, bc_{8i}$ are the 8 pixels of each input block Bc_i and $bc_{1o}, bc_{2o}, bc_{3o}, bc_{4o}, bc_{5o}, bc_{6o}, bc_{7o}, bc_{8o}$ are the corresponding 8 pixels of each output block Bc_o . The 8 pixels of the each output block Bc_o are given by the following equations:

$$bc_{2o} = \left[(bc_{2i})^{<<<r1} \right] \oplus k_2 \oplus bc_{3i} \tag{17}$$

$$bc_{3o} = bc_{4i} \oplus k_3 \oplus bc_{3i} \tag{18}$$

$$bc_{4o} = \left[(bc_{4i})^{<<<r2} \right] \oplus k_4 \oplus bc_{5i} \tag{19}$$

$$bc_{5o} = bc_{6i} \oplus k_5 \oplus bc_{5i} \tag{20}$$

$$bc_{6o} = \left[(bc_{6i})^{<<<r3} \right] \oplus k_6 \oplus bc_{7i} \tag{21}$$

$$bc_{7o} = bc_{7i} \oplus k_7 \oplus bc_{6i} \tag{22}$$

$$bc_{8o} = \left[(bc_{8i})^{<<<r4} \right] \oplus k_8 \oplus bc_{1i} \tag{23}$$

$$bc_{1o} = k_1 \oplus bc_{2i} \oplus bc_{2o} \oplus bc_{3o} \oplus bc_{4o} \oplus bc_{5o} \oplus bc_{6o} \oplus bc_{7o} \oplus bc_{8o} \tag{24}$$

4. Join the output bocks Bc_o of the 2nd round to form a matrix of size $(1 \times MN)$, then reshape it into $M \times N$ matrix to obtain the plain image P

4 Performance analysis and simulation results

The laptop used is Intel(R) Core(TM) i5-6200UCPU@2.30GHz, 4GB RAM, Windows 10 (64-bit), MATLAB 2017a. The proposed scheme is applied to Lena, Cameraman, Baboon and Airplane images all of size 256×256 . The results are given in Fig. 6. It is noted that our scheme converts the original images (as in Fig. 6a-d) into a nearly random encrypted images (Fig. 6e-h). While the decrypted images (Fig. 6i-l) are the same as the original images (Fig. 6a-d).

4.1 Numerical example

An explanation numerical example for Lena (256×256) grayscale image encryption will be considered in this section:

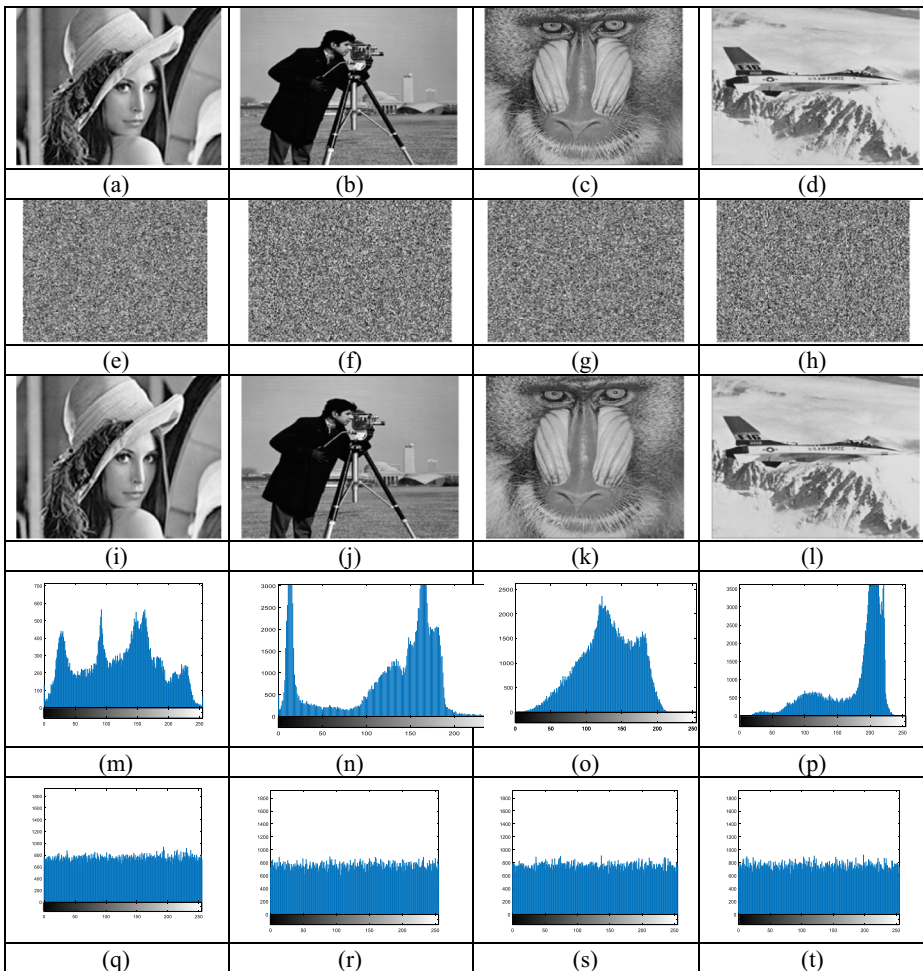


Fig. 6 Simulation results: **a** Lena; **b** Cameraman; **c** Baboon; **d** Airplane image; **e-h** Corresponding encrypted images of (a)-(d); **i-l** Corresponding decrypted images of (e)-(h); **m-p** corresponding histograms of (a)-(d); **q-t** corresponding histograms of (e)-(h)

1. Firstly, the hash function H of the Lena image is computed using SHA-512 as:

$H = \text{a68f82367bb3fa}ff26893059185417909\text{a3656cc7c8f52922310800217a74104ecc38d7a672914a00d}$
 $c770d01362aff5cd3a91053c6e8bd0ea17e105f1be6acd$

Convert H to decimal digits sequence then pad it with zeros to be multiple of 4 then divide the padded sequence into 4 equal length sequences $\{h_1, h_2, \dots, h_4\}$.

Compute the 4 values of the shift rotations using Eq. (4).

2. Select appropriate values for μ , k and z_0 for the proposed DCPG where

$$\mu = 0.399, k = 5.782595812953629 \text{ and } z_0 = 0.234$$

which generates a chaotic sequence of length 65,536 known as

$z = \{0.10858, -0.45069, 0.23039, \dots, -0.51860, 0.04314, -0.66262\}$ using Eq. (3) then convert this floating point sequence z into an integer sequence in the range $[0, 255]$, $C = \{173, 30, 131, \dots, 243, 188, 8\}$, using the Eq. (6) and divide it into 8192 blocks, each of size 1×8 .

3. Read Lena image as a 256×256 matrix of pixels. Reshape this matrix into a $1 \times 65,536$ one, and then divide it into blocks of size 1×8 .
4. The blocks of Lena image and the corresponding blocks of the DCPG with the four shift rotations are processed by the function in Fig. 5.
5. Join the output blocks of the first round to form a matrix of size $(1 \times 65,536)$, then reshape it into another one of size (8192×8) , with number of row = 8192 and number of columns = 8 then apply the function in Eq. 14 to each row. Finally reshape the output matrix into a 256×256 matrix to obtain the cipher image shown in Fig. 6e. Then recover the original plain image by reversing the steps of encryption.

The validity of our scheme will be proved using histogram, entropy, correlation coefficient, NPCR, UACI, PSNR, MDMF and key space properties.

4.2 Histogram analysis

Digital image pixel intensities distribution is graphically known as histogram and it is unique for each image (as shown in Fig. 6m-p). This makes it subject to statistical attacks. For a robust encryption, the encrypted image has to have nearly uniform distribution or be fairly flat (as shown in Fig. 6q-t). So our scheme has a good robustness against statistical attacks.

4.3 Correlation analysis

Generally, the pixels of a digital image are highly correlated. So a robust encryption has to be able to break this correlation to resist statistical attack.

If N pairs of adjacent pixels of the tested images with grayscale values as (x_i, y_i) , $i = 1, 2, \dots, N$ are randomly selected. The correlation coefficients between $x = \{x_i\}$

Table 2 Correlation coefficients of the tested images

Image	Direction	Plain image	Cipher image
Lena	Horizontal	0.9882	0.0029
	Vertical	0.9446	-0.0012
	Diagonal	0.9616	0.0010
Cameraman	Horizontal	0.9592	-0.0020
	Vertical	0.9074	-0.0025
	Diagonal	0.9330	-0.0101
Baboon	Horizontal	0.7844	-0.0043
	Vertical	0.7411	-0.0025
	Diagonal	0.8426	0.0014
Airplane	Horizontal	0.9209	-0.0029
	Vertical	0.8636	-0.0008
	Diagonal	0.9236	-0.0012

and $y = \{y_i\}$ is given by the equation:

$$\frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}} \tag{25}$$

Where, $E(x)$ represents the expected value of x .

For the proposed scheme, a randomly selected $N = 4096$ pairs of adjacent pixels in the horizontal, vertical, and diagonal directions of the tested images will be considered. Their correlation coefficients are calculated and listed in Table 2. Figure 7 indicates the correlation of Lena and its encrypted image in the three directions. From Table 2, we find the correlation coefficients between adjacent pixels in the original images a-d close to 1, while the correlation coefficients between adjacent pixels

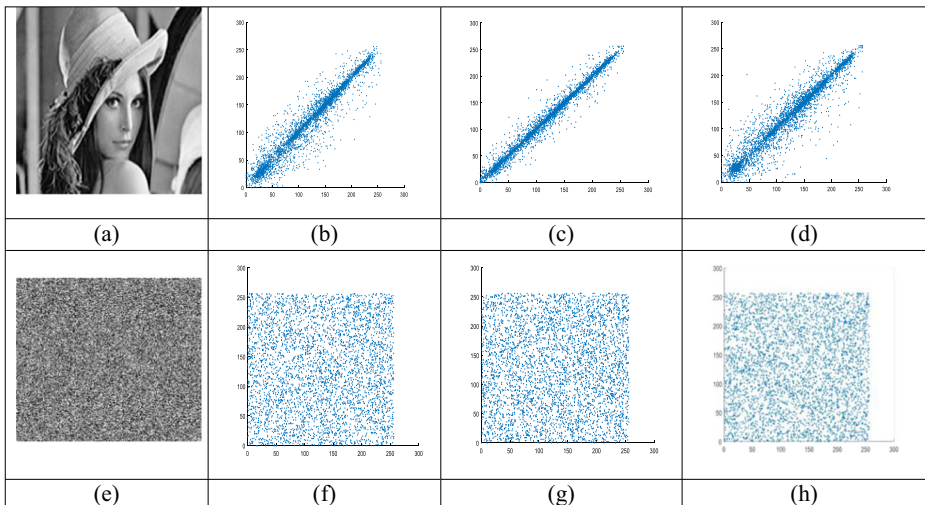


Fig. 7 Correlation Coefficient: **a** Lena; **b** Lena horizontal correlation; **c** Lena vertical correlation; **d** Lena diagonal correlation; **e** Cipher image of Lena; **f** Cipher image horizontal correlation **g** Cipher image vertical correlation; **h** Cipher image diagonal correlation

Table 3 Entropy of tested images

Lena		Cameraman		Baboon		Airplane	
Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
7.8066	7.9977	7.1048	7.9966	7.2687	7.9971	6.7866	7.9963

in the encrypted images e-h close to 0 which means that the adjacent pixels in encrypted images are uncorrelated and hence our scheme is strong against correlation analysis attack.

4.4 Entropy analysis

The entropy of an image measures the randomness of its pixels as:

$$H = \sum_{i=0}^L p(i) \log_2 p(i) \quad (26)$$

Where, L is the number of grayscale levels of images, and $p(i)$ is the probability of the gray value i occurrence. For an ideal random image, the maximum value of entropy is 8. Generally larger entropy value of cipher image means better encryption scheme. Table 3 indicates the entropy values of the tested original images and their corresponding encrypted images. From this table, the entropy values of the encrypted images are close to 8, so the encrypted images can resist the entropy analysis attack.

4.5 NPCR and UACI analysis

Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) can be used for measuring the effect of a single pixel change on the whole encrypted image and are defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (27)$$

$$UACI = \frac{1}{M \times N} \frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)|}{L} \times 100\% \quad (28)$$

Where $C_1(i,j)$ and $C_2(i,j)$ are the values of the pixels in the position (i,j) of the two cipher – images C_1 and C_2 respectively; L is the number of gray levels. $D(i,j)$ is given by the following equation:

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & otherwise \end{cases} \quad (29)$$

Table 4 NPCR and UACI of the tested images

	Lena	Cameraman	Baboon	Airplane
NPCR	100%	100%	100%	100%
UACI	35.66%	36%	47%	40.8%

Table 5 PSNR of the tested images

	Lena	Cameraman	Baboon	Airplane
PSNR	8.43	8.39	9.69	8.01

The theoretical values of NPCR and UACI are 99.61% and 33.46%, respectively. The higher their values are, the better the encryption. To measure these values for our scheme, a pixel was chosen randomly and change it value, then by using the encrypted image of the original image C_1 and the encrypted image of the modified image C_2 for computing NPCR and UACI for the tested images and listed it in Table 4.

4.6 PSNR (peak signal to noise ratio) analysis

PSNR is a good measure of the degradation of an image after encryption. It is given by the following equation:

$$PSNR = 20 \times \log_{10} \left(\frac{255}{\sqrt{MSE}} \right) \tag{30}$$

$$MSE = \frac{1}{W \times H} \sum_{i,j} (IC_1(i,j) - IC_2(i,j))^2 \tag{31}$$

Where $IC_1(i,j)$ is the original image pixel intensity at the index (i,j) . $IC_2(i,j)$ is the cipher image pixel intensity.

Better security can be achieved with PSNR value of encrypted images less than 10 dB. Table 5 shows the images PSNR. All PSNR values are below 10 dB.

4.7 Maximum deviation measuring factor (MDMF)

MDMF is another measure of the quality of an image encryption. A good image encryption maximizes the deviation between the original image and its corresponding cipher image. MDMF can be calculated as follows:

Firstly for an image of size $M \times N$, histogram of both the original and encrypted image is determined, then the absolute difference between these two values is calculated (D_i at the gray level i). Finally, the area under the absolute difference curve is divided by the total area to give MDMF as in the following equation:

$$MDMF = \frac{\left(\frac{D_1 + D_{256}}{2} + \sum_{i=2}^{255} d_i \right)}{M \times N} \tag{32}$$

The higher the MDMF is, the more secure the encryption. Table 6 shows the MDMF of the tested images.

Table 6 MDMF of the tested images

	Lena	Cameraman	Baboon	Airplane
MDMF	1.99	2.80	2.48	3.04

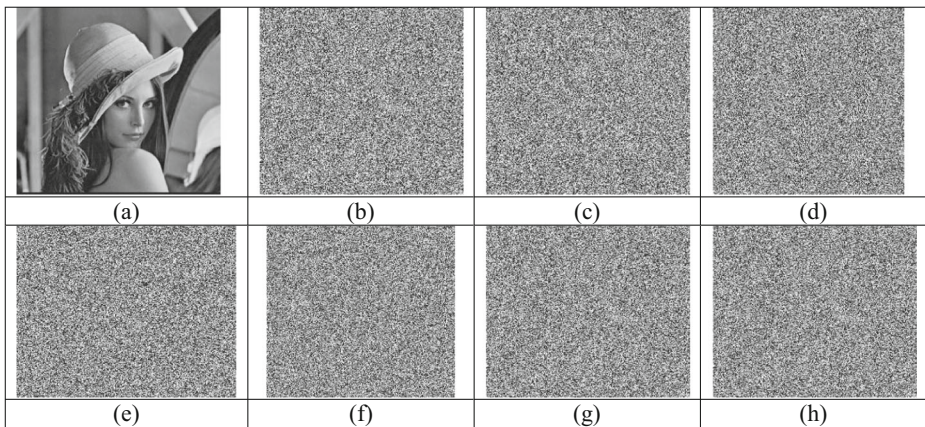


Fig. 8 Key sensitivity test

4.8 Key sensitivity test

In a good image encryption scheme, changing one bit in the secret key results in a totally different encrypted image. For our proposed scheme, a single bit change is made in each one of the three control parameters of the chaotic sequence generator, μ , k , z_0 which are secret values known only to the communicating entities to test its effect on the cipher images. Figure 8a is Lena image while Fig. 8b is its cipher image, with $\mu = 0.399$, $k = 5.782595812953629$ and $z_0 = 0.234$. Figure 8c represents the cipher image of Lena with changing k to 4.782595812953629. Figure 8d represents the cipher image of Lena with changing μ to 0.398. Figure 8e represents the cipher image of Lena with changing z_0 to 0.254.

The decrypted images in case of changing the secret keys, k , z_0 , μ are in Fig. 8f-h respectively. It is obvious that the decryption with a little key change fails to recover the original plain image. So our proposed scheme is very key sensitive.

Table 7 listed the correlations coefficient between the cipher image of Lena (Fig. 8b) and the cipher images with a little change in the secret keys, k , z_0 , μ (as shown in Fig. 8c-d and (e) respectively). According to this table, the encrypted images are uncorrelated.

4.9 Key space

Large key space achieves more robust encryption scheme against the brute force attack. For our scheme, there are four secret values: the three control parameters μ , k , z_0 of the chaotic sequence generator and 512 bit original image hash value. From which the shift rotations are computed. From the IEEE floating point standard the data precision for the double values is

Table 7 Correlation coefficient with a little key change

Image 1	Image 2	Correlation coefficient
Figure 8b	Figure 8c	-0.010366
	Figure 8d	-0.001319
	Figure 8e	-0.004434

Table 8 Key space compared with other schemes

	Ref [15]	Ref [58]	Ref [18]	Ref [63]	Ref [22]	Ref [57]	Ours
Key space size	2^{256}	2^{210}	2^{240}	10^{70}	2^{128}	2^{128}	2^{600}

10^{-15} . So the key space of our scheme = $2^{512} \times 10^{15} \times 10^{15} \times 10^{15} \cong 2^{600}$ which is extremely large, so our scheme is very strong against brute force attack compared to other scheme as shown in Table 8.

5 Comparison analysis

The performance of our scheme will be validated. Table 9 compares of the simulation results of our scheme with other recent encryption schemes.

Also, the proposed scheme has been tried on images of different size, and a comparison of entropy, encryption time and saving in time compared to AES [2] and the algorithm in Ref [15] is shown in Table 10. From this comparison, it is obvious that our scheme has much lower execution time and higher efficiency than both AES [2] and the algorithms in Ref [15, 17, 45].

6 Conclusions

An XOR, shift rotations and double chaotic pseudorandom generator (DCPG) based image encryption scheme has been introduced in this paper. DCPG combines both Tent and Chebyshev chaotic map and so it needs more control parameters. These parameters are used as shared secret keys between the sender and receiver. This increases the key space of the proposed scheme and so increases its strength against different types of attacks. Also, the amounts of shift rotation used depend on the input image which provides a strong resistance against chosen plaintext attacks. Due to these reasons, our scheme is highly secure. It consists only of two rounds of processing which makes it light weight and has lower execution time compared to other standard and recent schemes. The proposed scheme has been tried on images of different size. A comparison of encryption time of our scheme with AES shows that our scheme achieves time saving of 71.84%, 94.63%, 97.12% and 95.34% in case of image size of (64×64) , (256×256) , (320×320) and (512×512) respectively. It also has proved that our scheme achieves better efficiency than other recently existing schemes. So

Table 9 Performance comparison

Metrics	Ref [58]	Ref [18]	Ref [63]	Ref [22]	Ref [15]	AES [2]	Ours
Entropy	7.9974	7.9975	7.9994	7.9990	7.9978	7.9972	7.9977
Correlation between plain image & cipher image	0.0094	0.0087	0.0014	0.0073	0.0015	0.0019	0.0014
NPCR	99.62	99.519	99.616	100	99.639	99.644	100
UACI	33.51	33.58	33.43	33.55	27.77	27.79	35.66
MDFM	-	-	-	-	0.7872	0.7891	1.99

Table 10 Time comparison

Image size		Ref [15]	Ref [17]	Ref [45]	AES	Ours
(64 × 64)	Entropy	7.9329	-	-	2.7574	7.9571
	Encryption time (sec)	2.1	-	-	1.03	0.29
	Time saving (%) to AES	-	-	-	-	71.84%
	Time saving (%) to Ref [15]	-	-	-	50.95%	86.19%
(256 × 256)	Entropy	7.9978	-	7.9972	7.9972	7.9972
	Encryption time (sec)	7.44	5.55679	7.73	26.86	1.44
	Time saving (%) to AES	72.3%	79.3%	71.2%	-	94.63%
	Time saving (%) to Ref [15]	-	%25.3	-	-	80.64%
	Time saving (%) to Ref [17]	-	-	-	-	74.1%
	Time saving (%) to Ref [45]	3.75%	-	-	-	81.37%
(320 × 320)	Entropy	7.9941	-	-	7.4464	7.9966
	Encryption time (sec)	21.86	-	-	59.11	1.7
	Time saving (%) to AES	63%	-	-	-	97.12%
	Time saving (%) to Ref [15]	-	-	-	-	92.22%
(512 × 512)	Entropy	7.9993	7.9986	7.9991	7.9993	7.9993
	Encryption time (sec)	85.56	8.97439	31.59	116.24	5.41
	Time saving (%) to AES	26.39%	92.27%	72.82%	-	95.34%
	Time saving (%) to Ref [15]	-	89.5%	63.1%	-	93.68%
	Time saving (%) to Ref [17]	-	-	-	-	39.72%
	Time saving (%) to Ref [45]	-	71.68%	-	-	82.87%

our scheme is very suitable for real time secure image communications. For the future work, more secure pseudorandom generators with new chaotic maps and more control parameters can be proposed.

References

1. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based steganography using truth table based and determinate Array on RGB Indicator. *Int J Signal Image Process (IJSIP)* 1(3):196–204
2. Advanced Encryption Standard (AES) (2001) Federal Information Processing Standards Publication 197
3. Ahmad M, Shamsi U, Khan I (2015) An enhanced image encryption algorithm using fractional chaotic systems. *Proc Comput Sci* 57:852–859
4. Alanizy N, Alanizy A, Baghoza N, AlGhamdi M, Gutub A (2018) 3-layer PC text security via combining compression, AES cryptography 2LSB Image steganography. *J Res Eng Appl Sci (JREAS)* 3(4):118–124
5. Alassaf N, Alkazem B, Gutub A (2017) Applicable light-weight cryptography to secure medical data in IoT systems. *Journal of research in engineering and applied sciences (JREAS)* 2(2):50–58
6. Alassaf N, Gutub A, Parah S, Al Ghamdi M (2018) Enhancing speed of SIMON: a light-weight-cryptographic algorithm for IoT applications. *Multimedia tools and applications: an international journal - springer*, ISSN 1380–7501. <https://doi.org/10.1007/s11042-018-6801-z>
7. Al-Ghamdi M, Al-Ghamdi M, Gutub A (2018) Security enhancement of shares generation process for multimedia counting-based secret-sharing technique. *Multimedia tools and applications*, ISSN 1380–7501. <https://doi.org/10.1007/s11042-018-6977-2>
8. Al-Juaid N, Gutub A, Khan E (2018) Enhancing PC data security via combining RSA cryptography and video based steganography. *Journal of information security and cybercrimes research (JISCR)*, Vol. 1, no. 1, published by Naif Arab University for Security Sciences (NAUSS)
9. Almazroie M, Samsudin A, Gutub A, Salleh MS, Omar MA, Hassan SA (2018) Integrity verification for digital holy Quran verses using cryptographic hash function and compression. *Journal of King Saud University - Computer and Information Sciences*, Published by Elsevier, Published online: 8

10. Alsaidi A, Al-lehaibi K, Alzahrani H, AlGhamdi M, Gutub A Compression multi-level, crypto stego security of texts utilizing colored email forwarding. *J Comput Sci Comput Math (JCSCM)* 8(3):33–42. <https://doi.org/10.20967/jcscm.2018.03.002> Published by Science & Knowledge Research Society, September 2018
11. Alsmirat MA, Al-Alem F, Al-Ayyoub M, Jaraweh Y, Gupta B (2017) Impact of digital fingerprint image quality on the fingerprint recognition accuracy. *Multimed Tools Appl* 78(3):3649–3688, Springer
12. AlZain M, Faragallah O (2017) Efficient chaotic tent map-based image cryptosystem. *Int J Comput Appl* (0975–8887) 167(7)
13. Ansari S, Gupta N, Agrawal S (2012) An image encryption approach using chaotic map in frequency domain. *Int J Emerg Technol Adv Eng* 2(8):287–291
14. Asghar MN, Kousar R, Majid H, Fleury M (2017) Transparent Encryption with Scalable Video Communication: Lower-Latency, CABAC-Based Schemes. *J Vis Commun Image R, Elsevier* 45:122–136
15. Ayoup A, Hussein A, Attia M (2016) Efficient selective image encryption. *Multimed Tools Appl*. Springer Science+Business Media New York
16. Chai X, Gan Z, Yang K, Chen Y, Liu X (2017) An Image encryption algorithm based on the Memristive Hyperchaotic system, cellular automata and DNA sequence operations. *Signal Process: Image Commun Elsevier* 52:6–19
17. Chen J, Yu Z, Lin Q, Chong F, Xu L (2017) Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression. *Opt Laser Technol* 99:238–248
18. Enayatifar R, Abdullah A, Isnin I, Altameem A, Lee M (2017) Image encryption using a synchronous permutation-diffusion technique. *Opt Lasers Eng* 90:146–154
19. Eom S, Ho Huh J (2018) Group signature with restrictive linkability: minimizing privacy exposure in ubiquitous environment. *J Ambient Intell Humaniz Comput* : 1–11
20. Eom S, Ho Huh J (2018) The opening capability for security against privacy infringements in the smart grid environment. *Mathematics* 6.10:202
21. Essaid M, Akharraz I, Saaidi A, Mouhib A (2018) A new Image encryption scheme based on confusion-diffusion using an enhanced skew tent map, the first international conference on intelligent computing in data sciences; ScienceDirect, Elsevier. *Proc Comput Sci* 127:539–548
22. Essaid M, Akharraza I, Saaidi A, Mouhib A A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map, the first international conference on intelligent computing in data sciences. *Proc Comput Sci* 127(2018):539–548 Elsevier
23. Gupta BB (2018) Computer and cyber security: principles, algorithm, applications, and perspectives. CRC Press, Taylor & Francis, 666
24. Gupta P, Gupta A Image encryption based on 2D baker map and 1D logistic map. *Int J Adv Res Comput Sci Softw Eng* 7, 6, June 2017, pp: 499–503.
25. Gupta BB, Agrawal D, Yamaguchi S (2016) Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global
26. Gutub A (2010) Pixel Indicator technique for RGB Image steganography. *J Emerg Technol Web Intell (JETWI)* 2(1):56–64
27. Gutub A, M. Al-Ghamdi (2019) Image based steganography to facilitate improving counting-based secret sharing. *3D Research - Springer* 10(1). ISSN 2092–6731. <https://doi.org/10.1007/s13319-019-0216-0>
28. Gutub A, Al-Juaid N (2018) Multi-bits stego-system for hiding text in multimedia images based on user security priority. *J Comput Hardware Eng* 1(2). <https://doi.org/10.63019/jche.v1i2.513>, EnPress Publisher
29. Hua Z, Zhou Y (2016) Image encryption using 2D logistic-adjusted-sine map. *Inform Sci, Elsevier* 339: 237–253
30. Huang X (2012) Image encryption algorithm using chaotic chebyshev generator. *Nonlinear Dyn Springer* 67(4):2411–2417
31. Hung X (2012) Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dyn* 67:2411–2417
32. Jyoti S, Bowade PK, Raghuvansh MM (2015) Technique of video encryption /scrambling using chaotic functions and analysis. *J Emerg Technol Innov Res* 2(6):1951 - 1958
33. Kadir A, Hamdulla A, Guo W (2014) Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik-Int J Light Electron Optics* 125(5):1671–1675
34. Kong D, Cao L, Shen X, Zhang H, Jin G (2018) Image encryption based on interleaved computer-generated holograms. *IEEE Trans Industr Inform* 14(2):673–678
35. Kumar M, Kumar S, Budhiraja R, Das MK, Singh S (2016) Intertwining logistic map and Cellular Automata based color image encryption model. *Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on* (pp. 618–623). IEEE

36. Li C, Luo G, Qin K (2017) An image encryption scheme based on chaotic tent map. *Nonlinear Dyn* 87:127–133 © Springer science+business media Dordrecht 2016
37. Madhuravani B, Murthy DSR (2017) A hybrid parallel hash model based on multichaotic maps for mobile data security. *J Theor Appl Inform Technol JATIT & LLS* 95(3):661–669
38. Mahmood A, Dony R, Areibi S (2013) An adaptive encryption based genetic algorithms for medical images
39. Murillo Escobar MA, Cardoza L, Lopez-Gutierrez RM, Cruz-Hernandez C (2017) A double chaotic layer encryption algorithm for clinical signals in telemedicine. *J Med Syst* 41(4):59
40. Murillo-Escobar M, Hernandez C (2017) A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dyn* 87(1):407–425
41. Naveenkumar S, Panduranga H (2013) Partial image encryption for smart camera", machine learning for signal processing (MLSP). *IEEE international workshop, international conference on recent trends in information technology (ICRTIT)*: 126–132
42. Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. *Signal Process* 138:129–137
43. Pareschi F, Rovatti R, Setti G (2012) On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Trans Inform Forensics Sec* 7(2):491–505
44. Ponuma R, Amuth R (2018) Compressive sensing based image compression-encryption using novel 1D-chaotic map. *Multimed Tools Appl*. Springer 77(15):19209–19234
45. Reham AU, Liao X, Kulsoom A, Abbas ASA (2015) Selective encryption for gray images based on chaos and DNA complementary rules. *Multimed Tools Appl* 74(13):4655–4677
46. Rogaway P, Shrimpton T (2004) Cryptographic hash-function basics: definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. *J Fast Softw Encrypt* 3017:371–388
47. Rostami MJ, Shahba A, Saryazdi S, Nezamabadi-pour H (2017) A Novel Parallel Image encryption with chaotic windows based on logistic map. *Comput Electric Eng Elsevier* 62:384–400
48. Sam S, Devaraj P, Bhuvaneshwaran R (2012) An intertwining chaotic maps based image encryption scheme. *Nonlinear Dyn* 69(4):1995
49. Sheela S, Sathyanarayana SV (2016) Application of Chaos theory in data security-a survey. *ACCENTS Trans Inform Sec Proc National Workshop on Cryptol* 2(5):1–15
50. Sufi F, Han F, Khalil I, Hu J (2011) A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications. *Sec Commun Netw* 4.5:515–524
51. Tang J, Zhang F (2017) A new code-based encryption scheme and its applications. *Int J High Perform Comput Netw* 10.6:515–523
52. Tanvir M, Gutub A (2011) Vibrant color Image steganography using channel differences and secret data distribution. *Kuwait J Sci Eng (KJSE)* 38(1B):127–142
53. Wang J, Wang C (2018) Full secure identity-based encryption scheme over lattices for wireless sensor networks in the standard model. *International Journal of High Performance Computing and Networking* 12(2). <https://doi.org/10.1504/IJHPCN.2018.094361>
54. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on Chaos. *Signal Process* 92:1101–1108
55. Wu Y, Yang G, Jin H, Noonan JP (2012) Image encryption using the two-dimensional logistic chaotic map. *J Electron Imag*
56. Wu X, Zhu B, Hu Y, Ran Y (2017) A Novel color Image encryption scheme using rectangular transform-enhanced chaotic tent maps. *IEEE Access* 5:6429–6436
57. Xing Y, Li M, Wang L (2018) Chaotic-map Image Encryption Scheme based on AES Key Producing Schedule. 2018 IEEE Third International Conference on Data Science in Cyberspace
58. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. *Opt Lasers Eng* 78:17–25
59. Ye G, Huang X (2016) A secure image encryption algorithm based on chaotic maps and SHA-3. *Sec Commun Netw* 9.13:2015–2023
60. Ye G, Zhou J (2014) A block chaotic image encryption scheme based on self-adaptive modelling. *Appl Soft Comput* 22:351–357
61. Yoon E, Jeon I (2011) An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map. *Commun Nonlinear Sci Numer Simul* 16:2383–2389
62. Zhang J, Gao H (2019) A compact construction for non-monotonic key-policy attribute-based encryption. *Int J High Perform Comput Netw* 13.3:321–330
63. Zhang Y, Xiao D (2014) An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Commun Nonlinear Sci Numer Simul* 19(1):74–82
64. Zhou Y, Bao L, Chen C (2014) A new 1D chaotic system for image encryption. *Signal Process* 97:172–182

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



Dr. Roayat Ismail Abdelfatah received a BSc. Degree in Electronics and Electrical communications engineering department from Tanta university, Egypt in 2000 and received her M. Sc. and Ph. D. degrees from Tanta university in 2005 and 2011, respectively. Her M. Sc. is dedicated in encryption techniques and its applications. The Ph. D. is devoted to introduce new encryption, digital signature, signcryption and hash functions algorithms for securing digital data over communication networks.