Complex & Intelligent Systems (2023) 9:4817–4835
https://doi.org/10.1007/s40747-023-00988-7

ORIGINAL ARTICLE

Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem

Bassem Abd-El-Atty[1]

Received: 4 August 2022 / Accepted: 22 January 2023 / Published online: 15 February 2023

Abstract
Amidst the growth of the internet and communication technologies, the requirements for the security of data transmitted via these technologies are increasing. Visual data, like images and videos, are commonly utilized for representing the majority of data due to its having more detailed information. Until now, the physical implementation of quantum computers does not have enough capability for hacking any traditional image cryptosystem, but amidst the growth of quantum resources, enough capability may be available in the near future. Most data represented by images has a long lifetime, like personal, medical, military, etc. Therefore, new quantum-inspired-based designs for image cryptosystems are required to be performed on digital resources and have the capability of defying the potential attacks from digital and quantum resources. In this study, a new substitution box (S-box) mechanism is proposed, which is based on quantum-inspired quantum walks, Hénon map, and a customized particle swarm optimization algorithm. Performance analysis of the suggested S-box proves its effectiveness and its reliability in designing various cryptosystems. Based on the effectiveness of the presented S-box, a new image cryptosystem is proposed, in which its experiential outcomes prove its efficacy and security against various attacks. The average outcome of entropy is 7.99977, UACI is 33.484%, NPCR is 99.618%, and Chi-square is 249.481 for the constructed cipher images.

Keywords Data security · Quantum walks · Quantum-inspired models · PSO · Hénon map · Substitution box · Image encryption

Introduction

Data security plays an essential task in daily life because of the increasing growth of the internet and communication technologies. Visual data, like images and videos, are commonly utilized for representing the majority of data due to its having more detailed information. Digital images can be secured during the transmission and storing process on local or cloud storage via utilizing one of several image data hiding or image cryptosystems [1,2]. The main aim of image cryptosystems is to transform the image from a recognizable style to an unrecognizable format. There are many tools utilized in designing modern image cryptosystems, like chaotic maps, S-boxes, cellular automata, DNA, etc. [3–5].

Any well-designed image cryptosystem has mainly three phases: (1) key generation, which is related to the pristine image; (2) confusion; and (3) diffusion. In addition to their main role in the diffusion process, S-boxes may be utilized as permutation boxes for fulfilling the confusion process. Recently, chaotic systems have been commonly utilized as a primary tool for constructing S-boxes because of their chaotic behavior, ease of implementation, and sensitivity to control parameters and primary conditions [6,7].

Motivation

Optimization algorithms play an essential role in constructing S-boxes to gain secure S-boxes with good nonlinearity [8, 9]. However, the role of optimization algorithms is to select a well-constructed S-box based on its performance analyses, not to utilize optimization algorithms in designing S-box mechanisms. Correspondingly, optimization algorithms play an essential role in developing image cryptosystems to gain secure cipher images with good cryptographic properties [10,11]. However, the role of optimization algorithms is to select a well-constructed cipher image based on its performance analyses, not to utilize optimization algorithms

✉ Bassem Abd-El-Atty
bassem.abdelatty@fci.luxor.edu.eg

[1] Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt

in designing image cryptosystems. Optimization algorithms include particle swarm optimization (PSO) [12], artificial bee colony [13], ant colony optimization [14], and others, with the PSO algorithm having a low computational time, being simple to execute due to it does not need a large number of parameters, and having a high confluence rate. PSO focuses on a small number of random particles and uses recurrence to find an effective solution. Therefore, Luo et al. [15] utilized the benefits of the PSO algorithm and customized it to perform as a chaotic system for designing a novel image cryptosystem with good performance.

The physical implementation of quantum computers does not have sufficient capability for hacking any traditional cryptosystem yet, but amidst the growth of quantum resources, sufficient capability may be available in the near future and most digital cryptosystems may be breached because their design is based on mathematical models [16]. Therefore, some researchers are concerned with developing quantum algorithms for securing data in the quantum era [17]. However, most digital data have a long lifetime, like military, medical, personal, etc. Consequently, confidential data must be secured before powerful quantum computers are available for hacking these data. Based on the issues raised, we need to develop new cryptosystems with structures based on quantum-inspired models that can withstand possible assaults from both classical and quantum devices, and their structures are based on optimization techniques to provide extra security. Among quantum paradigms, there is a quantum walk (QW), which is a quantum computing model used in the development of quantum mechanisms and may be used as a quantum-inspired model for constructing current cryptosystems that can be run on both digital and quantum platforms.

Contribution

From the stated issues above, we present a new S-box whose design is based on quantum-inspired QW, Hénon map, and a customized PSO algorithm. In the suggested S-box approach, QW is utilized as a quantum-inspired model to be performed on digital resources, and the PSO algorithm is customized to be utilized in designing the proposed mechanism. Performance analysis of the presented S-box proves its effectiveness and its reliability in designing various cryptosystems. Based on the efficiency of the presented S-box, a new image cryptosystem is suggested. In the suggested image cryptosystem, the probability vector generated from operating quantum-inspired QW and the generated sequences from Hénon map are utilized to operate the customized PSO algorithm for generating two sequences (X and Y), in which X and Y sequences are utilized for constructing different two permutation boxes to shuffle columns and rows of the pristine image. Then, the X sequence is utilized for constructing an 8×8 S-box to substitute the pixels of the permutated image, while the Y sequence is utilized for generating a pseudo-random sequence to construct the cipher image from the substituted image. Experimental results of the suggested image cryptosystem prove its efficiency and security against various attacks.

The summary of the key contributions of this study is listed below:

1. This study opens the door to utilizing quantum-inspired models with optimization algorithms in designing S-boxes.
2. Designing a new S-box using quantum-inspired QW, Hénon map, and the customized PSO algorithm.
3. Performance analysis of the presented S-box proves its effectiveness and its reliability in designing various cryptosystems.
4. Suggesting a new image encryption approach using the presented S-box approach.
5. The presented encryption approach has a high sensitivity for both pristine image and key sensitivity.

Organization

The remnant of this study is scheduled as given: the recent works related to the presented study are discussed in the next section, while the preliminaries for QW, Hénon map, and the customized PSO algorithm are given in "Preliminaries". The suggested S-box approach and its performance are delivered in "Proposed S-box algorithm and its analyses", while the proposed image cryptosystem and its performance analyses are provided in "Proposed encryption algorithm" and "Experimental outcomes and analyses".

Related work

Visual data, like images and videos, are commonly utilized for representing the majority of data due to its having more detailed information. Digital images can be secured during the transmission and storing process on local or cloud storage via utilizing one of several image encryption techniques. Recently, chaotic systems have been commonly utilized as a primary tool for developing image cryptosystems because of their chaotic behavior, ease of implementation, and sensitivity to control parameters and primary conditions. For example, Wang and Gao [18] presented a new chaos-based image encryption approach using the semi-tensor product. In the presented cryptosystem, the plain image is splitted into 4 blocks at random, then utilize several rounds of Arnold cat map to scramble each block. Based on the logistic map, Rupa et al. [19] presented a new medical multimedia cryptosystem, but the presented cryptosystem suffers from plain image-sensitivity attacks. Using logistic map and a 2D chaotic system, Askar et al. [20] presented an image encryption algorithm, but the suggested approach does not achieve the sensitivity of the pristine image. Vaidyanathan et al. [21] introduced a new 4D hyperchaotic system and demonstrated its use in developing a new image cryptosystem.

Any well-designed image cryptosystem has mainly three phases: (1) key generation, which is associated with the original image; (2) confusion; and (3) diffusion. In addition to their main role in the diffusion process, S-boxes may be utilized as permutation boxes for fulfilling the confusion process. In [4], Naseer et al. presented an image encryption mechanism based on a 3D chaotic system, in which the permutation phase is based on a permutation box and the substitution phase is based on an S-box. However, plain image sensitivity is not achieved for the presented cryptosystem. Using a 1D chaotic system, Rehman et al. [22] offered a medical image cryptosystem for privacy-preserving the medical data during transmission before evaluating it for cancer detection, in which an S-box is used in the substitution phase of the encryption procedure. Recently, chaotic systems have been commonly utilized as a primary tool for constructing S-boxes because of their chaotic behavior, implementation easy, and parameters sensitivity and primary conditions. For example, Maazouz et al. [3] suggested a new 3D chaotic system and presented its purpose in constructing S-boxes and utilizing the generated S-box in designing a new image encryption scheme, but the final encrypted image is generated after several rounds of encryption. Based on a 3D chaotic system, El-Latif et al. [23] offered a new S-box construction algorithm and its application in designing a new image encryption scheme, in which the generated S-boxes are utilized in permutation and substitution phases. Also, El-Latif et al. [7] suggested a new 3D hyperchaotic system and presented its application in constructing S-boxes and utilizing the generated S-box in designing a new image cryptosystem. In [24], Belazi et al. presented a new approach for constructing S-boxes based on a 1D chaotic map and utilizing the generated S-box in designing a new image encryption scheme. Using the Latin square and a 1D chaotic map, Hua et al. [25] presented a new S-box construction algorithm and presented its purpose in designing an image encryption. Based on the Gingerbreadman chaotic system, Khan and Asghar [26] presented a new S-box construction algorithm.

Optimization algorithms play an essential role in constructing S-boxes to gain secure S-boxes with good nonlinearity. For example, Zamli [9] presented a new S-box construction based on the adaptive agent heroes and cowards (AAHC) algorithm and Tent map, in which the role of AAHC is to select a well-constructed S-box based on its strict avalanche criteria (SAC) and nonlinearity. Also, Zamli et al. [27] presented a new S-box construction algorithm based on selective chaotic maps, in which the Tiki-Taka algorithm is used to select a well-constructed S-box based on its nonlinearity. Based on a 1D chaotic map and the cuckoo search algorithm, Alhadawi et al. [28] presented a new S-box construction algorithm, in which the role of the cuckoo search algorithm is to select a well-constructed S-box based on its nonlinearity. In [29], Farah et al. integrated three 1D chaotic maps for the construction of a new chaotic system and presented its purpose in constructing S-boxes and utilized the Jaya optimization algorithm to select a well-constructed S-box based on its nonlinearity. Then, the newly constructed S-boxes are utilized for designing a new image cryptosystem. Based on the optimization of control parameters for 1D chaotic maps, Tanyildizi and Ozkaynak [30] presented a new S-box construction algorithm, in which the Chi-square value is utilized as the objective function of optimization algorithms. Based on ergodic chaotic map and improved PSO, Hematpour and Ahadpour [8] presented a new S-box construction algorithm, in which the task of the improved PSO is to pick a well-constructed S-box based on its nonlinearity and entropy. However, the role of optimization algorithms stated in [8,9,27–30] is to select a well-constructed S-box based on its performance analyses, not to utilize optimization algorithms in designing S-box mechanisms.

Likewise, optimization algorithms play an essential role in developing image cryptosystems to gain secure cipher images with good cryptographic properties. For example, based on the integration of PWLC and 2DLC maps and improved whale optimization, Saravanan and Sivabalakrishnan [10] presented an image cryptosystem in which the final cipher image is obtained by iterative improved whale optimization using the best values for information entropy. In [11], Noshadian et al. introduced an image encryption approach using evolutionary algorithms and the logistic map. The final cipher image is optimized using information entropy or correlation coefficient. Wang and Li [31] introduced an image encryption approach using PSO, DNA, and the logistic map, but the final cipher image is obtained by iterative PSO using the best values for information entropy and correlation coefficient. Using a 4D hyperchaotic map and PSO, Zeng and Wang [32] suggested an image encryption scheme in which the final cipher image is obtained by iterative PSO using the best values for correlation coefficients. In [33], Ahmad et al. suggested an image cryptosystem using PSO and the logistic map, but the final cipher image is obtained by iterative PSO using the best values for correlation coefficients. However, the role of optimization algorithms stated in [10,11,31–33] is to select a well-constructed cipher image based on its performance analyses, not to utilize optimization algorithms in designing image cryptosystems. To overcome this issue, Luo et al. [15] integrate PSO with a 4D hyperchaotic system for designing a new image cryptosystem.

The physical implementation of quantum computers doesn't have sufficient capability for hacking any traditional cryptosystem yet, but amidst the growth of quantum resources, sufficient capability may be available in the near future and the majority of digital cryptosystems may be cracked because their design is based on mathematical models. Therefore, some researchers are concerned with developing quantum algorithms for securing data in the quantum age. For instance, Jiang et al. [17] suggested an quantum image encryption scheme based on the Henon map, but the suggested encryption approach suffers from plain image-sensitivity attacks.

Most digital data have a long lifetime, like military, medical, personal, etc. Consequently, confidential data must be secured before the availability of sufficiently powerful quantum computers for hacking this data. Therefore, El-Latif et al. [34] suggested a new S-box approach using quantum walks as a quantum-inspired model and a 1D chaotic map. Then the presented S-box approach is utilized for designing a new image cryptosystem, but the presented cryptosystem suffers from plain image-sensitivity attacks. In [16], Abd-El-Atty et al. presented an image encryption algorithm for cloud applications using quantum-inspired QW model, Henon map, and Gray code, in which the final encrypted image is generated after two rounds of encryption.

Based on the issues raised, we need to design new cryptosystems with structures based on quantum-inspired models that can withstand possible assaults from both classical and quantum devices, and their structure is based on optimization techniques to bring extra security. Accordingly, Abd-El-Atty integrates PSO and quantum walks in [35] to develop a novel medical image steganography algorithm that uses PSO in the embedding process. Therefore, we need to apply this idea to developing new S-box algorithms and their applications in image cryptosystems.

Preliminaries

In this part, we present the preliminaries for QW, Hénon map, and the customized PSO algorithm that are needed for developing the proposed S-box approach.

Quantum walk

There are two main elements for QW: coin particle $H_c = \cos\theta|0\rangle + \sin\theta|1\rangle$ and walker space H_s [36]. In every step t of acting QW on a cycle of V-node governed by a binary message S, a unitary revolution $\hat{R}_1$ (or $\hat{R}_0$) is applied on the whole quantum system if the tth-bit of S is 1 (or 0), otherwise $\hat{R}_2$ is applied. The mathematical expression of $\hat{R}_1$ is as in Eq. (1),

$$\hat{R}_1 = \hat{H}(\hat{I} \otimes \hat{O}_1), \tag{1}$$

where $\hat{H}$ is the shift operator of running QW on a cycle of V-node and can be represented as follows:

$$\hat{H} = \sum_{j=0}^{V-1} (|(j-1) \mod V, 1\rangle\langle j, 1| + |(j+1) \mod V, 0\rangle\langle j, 0|) \tag{2}$$

and the coin operator $\hat{O}_1$ can be expressed as follows:

$$\hat{O}_1 = \begin{pmatrix} \cos\sigma_1 & \sin\sigma_1 \\ \sin\ \sigma_1 & -\cos\sigma_1 \end{pmatrix}, \tag{3}$$

where $\sigma_1 \in [0, \pi/2]$. Similar $\hat{R}_1$, $\hat{R}_0$ and $\hat{R}_2$ can be formed. After operating QW t steps, the probability of finding the particle at vertex j can be stated as in Eq. (4):

$$\mathrm{Prb}(j,t) = \left|\langle j, 0| \left(\hat{R}_c\right)^t |\varphi\rangle_0\right|^2 + \left|\langle j, 1| \left(\hat{R}_c\right)^t |\varphi\rangle_0\right|^2, \tag{4}$$

where $c \in \{0, 1, 2\}$ and $|\varphi\rangle_0$ is the original quantum state of QW.

Hénon map

Chaotic systems have been commonly utilized as a primary tool for constructing S-boxes and image cryptosystems because of their chaotic behavior, ease of implementation, and sensitivity to control parameters and primary conditions. Hénon map is a two-dimensional chaotic map and is expressed in Eq. (5):

$$\begin{cases} p_{j+1} = q_j - ap_j^2 + 1 \\ q_{j+1} = bp_j, \end{cases} \tag{5}$$

where p_0, q_0 are the primary conditions and $a = 1.4$, $b = 0.3$ are the control parameters of Hénon map. For more information about the chaotic Hénon map, go to Ref. [17].

Particle swarm optimization

Optimization algorithms play an essential role in constructing S-boxes to gain secure S-boxes with good nonlinearity. However, the role of optimization algorithms is to select a well-constructed S-box based on its performance analyses, not to utilize optimization algorithms in designing S-box mechanisms. Among optimization algorithms, there is the PSO algorithm, which has a low computational time, being simple to execute due to it does not need a large number of parameters, and having a high confluence rate. PSO focuses on a small number of random particles and uses recurrence to find an effective solution. In PSO, each particle represents an individual solution. Each particle k possesses an initial state, pbest (z_k), gbest (w_k), and two primary parts: velocity (x_k) and position (y_k), which are used to run the PSO algorithm. To update each particle's location and velocity, Eq. (6) can be utilized [37]:

$$\begin{cases} x_{k,j}(i+1) = \alpha x_{k,j}(i) + d1 \times u_j(i)(z_{k,j}(i) - y_{k,j}(i)) \\ \qquad\qquad +d2 \times v_j(i)(w_{k,j}(i) - y_{k,j}(i)) \\ y_{k,j}(i+1) = x_{k,j}(i+1) + y_{k,j}(i), \end{cases} \tag{6}$$

where i denotes the iteration number, k is the particle number, the particle's dimensions are j, α indicates the inertia coefficient, $d1$ is the subjective parameter, $d2$ is the collective parameter, and $u_j, v_j \in (0, 1)$ are random numbers.

To adapt the PSO algorithm to be employed in the designing process of the suggested S-box algorithm, we customized it as reported in [15]. The mathematical representation of the customized PSO algorithm is provided as follows:

$$\begin{cases} x_{i+1} = \alpha x_i + d1 \times u_i\,(z_i - y_i) + d2 \times v_i\,(w_i - y_i) \\ y_{i+1} = x_{i+1} + y_i, \end{cases} \tag{7}$$

where sequence $\{U\}$ is generated from running QW, and sequences $\{V\}$, $\{Z\}$, and $\{W\}$ are generated from iterating Hénon map.

Proposed S-box algorithm and its analyses

S-boxes are considered the backbone component of designing modern cryptosystems. Recently, chaotic systems have been commonly utilized as a primary tool for constructing S-boxes because of their chaotic behavior, ease of implementation, and sensitivity to control parameters and primary conditions. Also, optimization algorithms play an essential role in constructing S-boxes to gain secure S-boxes with good nonlinearity. However, the role of optimization algorithms in the constructed S-boxes is to select a well-constructed S-box based on its performance analyses, not to utilize optimization algorithms in designing S-box mechanisms. Amidst the growth of quantum resources, sufficient capability may be available in the near future and most S-boxes may be hacked. Based on the issues raised, we need to develop new S-box mechanisms based on quantum-inspired models that can withstand possible assaults from both classical and quantum devices, and their structures are based on optimization techniques to provide extra security. In this regard, we present a new S-box algorithm to fulfill the requirements mentioned above.

S-box algorithm

The suggested S-box algorithm is based on quantum-inspired QW, Hénon map, and the customized PSO algorithm, in which QW is utilized as a quantum-inspired model to be performed on digital resources, and the PSO algorithm is customized to be utilized in designing the proposed mechanism. The detailed steps of the suggested S-box algorithm are itemized in the following points.

Step 1: Set the initial values of parameters (S, V, t, θ, σ_0, σ_1, σ_2, p_0, q_0, a, b, α, $d1$, $d2$, x_0, y_0).

Step 2: Using S, V, t, θ, σ_0, σ_1, σ_2 operate QW for t steps on a circle of V-vertex as a quantum-inspired model, for producing a probability vector Prb of length V, then resize the elements of the Prb vector to another vector of length g, where g is the number of elements in the desired S-box

$$U = \text{resize}\left(\text{Prb}, \left[\, g \;\; 1 \,\right]\right). \tag{8}$$

Step 3: Using p_0, q_0, a, b iterate Hénon map for g times, and generating two chaotic sequences (P, Q) each of length g, then from these sequences generate three sequences as given below

$$V = P \mod 1, \tag{9}$$

$$Z = Q \mod 1, \tag{10}$$

$$W = (P - Q) \mod 1. \tag{11}$$

Step 4: Using parameters (α, $d1$, $d2$, x_0, y_0) and the generated sequences (U, V, Z, W) operate the customized PSO (7) for generating two sequences (X, Y) each of length g.

Step 5: Organize the elements of a sequence X from the smallest to the largest as a sequence A, then locate the index of per element of A in X as an S-box of g-element.

S-box performance analyses

To verify the efficiency of the offered S-box algorithm, several analyses performed for the constructed 8 × 8 S-box. The most crucial requirements for a robust S-box have been laid forth in [38]. Among these requirements, Bijectivity, NL ("nonlinearity"), SAC ("strict avalanche criterion"), BIC ("bit independence"), LP ("linear approximation probability"), and DP ("differential probability"). The key parameters that utilized for constructing the S-box stated in Table 1 are set as: S = [0100 0100 1011 1101 0101 0101 0110 1001 1010 0110 0101], $V = 265$, $t = 270$, $\theta = 0$, $\sigma_0 = \pi/3$, $\sigma_1 = \pi/4$, $\sigma_2 = \pi/6$, $p_0 = 0.6495$, $q_0 = 0.5073$, $a = 1.4$, $b = 0.3$, $\alpha = 0.1$, $d1 = 0.5$, $d2 = 0.5$, $x_0 = 0.5$, and $y_0 = 1$.

Table 1 The constructed 8 × 8 S-box

12	228	254	78	121	76	215	80	132	245	168	43	9	130	159	182
15	49	207	20	61	106	8	131	114	181	66	154	243	14	136	82
13	249	98	116	217	91	230	16	111	77	40	93	150	231	155	146
119	51	165	208	41	177	59	233	138	85	167	169	229	53	47	1
18	72	148	134	88	60	162	56	46	209	2	101	253	171	225	212
103	63	179	173	198	244	39	172	241	113	248	178	170	26	190	105
176	216	55	33	220	166	11	27	69	219	201	108	28	6	64	242
164	110	232	246	58	71	95	7	174	197	89	161	145	194	175	185
118	180	187	135	239	32	34	193	37	70	139	97	23	142	4	75
92	25	65	74	202	141	206	140	10	156	129	204	147	188	227	109
137	158	143	19	62	247	149	192	200	123	213	160	30	189	57	237
67	21	0	122	17	196	218	195	144	94	35	236	112	214	153	125
221	3	222	224	115	22	234	205	184	52	157	250	36	107	50	83
48	124	84	152	223	120	126	127	183	128	24	81	252	235	117	42
86	133	251	100	151	38	240	211	226	44	5	99	191	210	45	163
203	73	186	68	90	96	199	54	104	238	102	29	79	87	255	31

Table 2 Nonlinearities

S-box	NL		
	Min	Max	Average
Proposed	102	110	107.00
[39]	104	110	106.50
[24]	102	108	105.25
[29]	104	108	106.25
[25]	102	108	105.25
[23]	104	110	106.00

Table 4 Comparison of SAC

S-box	SAC		
	Min	Max	Avg
Proposed	0.3906	0.6094	0.5044
[39]	0.4531	0.5469	0.4995
[24]	0.4297	0.5313	0.4956
[29]	0.4453	0.5546	0.5009
[25]	0.4688	0.5938	0.5351
[23]	0.3750	0.5938	0.4993

Bijective characteristic

An $n \times n$ S-box is bijective if it has 2^n distinct integer and all in the range $[0, 2^n - 1]$. From the elements stated in Table 1, the provided S-box satisfies the bijective property.

Nonlinearity

The constructed S-box has nonlinearity scores of 108, 108, 108, 106, 102, 110, 106, and 108, respectively. The nonlinearities of our S-box and other S-boxes displayed in [23–25,29,39] are stated in Table 2, in which our constructed S-box has good average nonlinearity.

SAC

Table 3 displays the dependence matrix for the generated S-box. The average value of the generated dependence matrix is 0.5044, which is extremely close to the optimal value of 0.5000. Table 4 lists the max, min, and average values of

Table 3 Dependence matrix of the presented S-box

0.5625	0.5625	0.5313	0.4375	0.4531	0.5156	0.5781	0.5156
0.5000	0.4531	0.5469	0.4844	0.5469	0.5781	0.4844	0.4375
0.5156	0.4844	0.3906	0.5000	0.5469	0.5000	0.3906	0.4844
0.5000	0.5156	0.5781	0.5000	0.4531	0.5000	0.5469	0.6094
0.5000	0.4688	0.5156	0.4688	0.4375	0.4844	0.5156	0.5156
0.5313	0.5313	0.4531	0.5625	0.5156	0.5000	0.4375	0.5625
0.5781	0.4688	0.5469	0.4531	0.4844	0.4844	0.5000	0.4844
0.4844	0.6094	0.5313	0.4844	0.5313	0.4219	0.5469	0.4688

Table 5 BIC-nonlinearity of our S-box

–	106	102	100	102	98	108	104
106	–	102	104	102	102	104	104
102	102	–	106	104	104	104	106
100	104	106	–	108	100	104	102
102	102	104	108	–	104	100	96
98	102	104	100	104	–	104	104
108	104	104	104	100	104	–	100
104	104	106	102	96	104	100	–

the dependence matrix for our S-box and other S-boxes. The results show that our S-box has good SAC properties.

BIC

Tables 5 and 6 show the BIC results for our S-box. The BIC-nonlinearity is shown in Table 5 with an average value of 103. According to Table 6, the BIC-SAC average is 0.5066, which is extremely close to the ideal value of 0.5000. Therefore, the constructed S-box satisfies the BIC criteria. The results from our S-box provide a realistically acceptable range, as shown by a comparison of the nonlinearities of BIC and BIC–SAC in Table 7.

Differential approximation probability

Table 8 shows the differential approximation values for the constructed S-box. The presented approach is robust against differential assaults, as shown by the DPs values of the constructed S-box, which is 0.03125. Table 9 provides the PDs of different S-boxes, and our S-box has an acceptable DP value when compared to other S-boxes.

LP

Table 10 provides the probability of linear approximation for our S-box with other S-boxes. As a result, the constructed S-box exhibits acceptable LP properties.

Table 7 Comparison of BIC

S-box	Avg. BIC-nonlinearity	Avg. BIC–SAC
Proposed	103.00	0.5066
[39]	104.57	0.4983
[24]	103.80	0.4996
[29]	103.64	0.4996
[25]	103.21	0.5000
[23]	104.21	0.5030

Table 8 DP for our S-box

8	8	6	8	10	6	8	8	6	8	6	8	6	6	6	6
8	6	6	8	6	8	8	6	6	6	6	8	6	6	6	6
6	8	8	6	6	8	6	8	6	6	8	8	6	6	6	6
6	6	6	6	6	8	6	6	6	6	8	6	8	6	8	6
6	8	6	4	8	10	6	8	6	6	8	8	6	6	6	6
10	8	6	6	6	6	6	8	8	8	10	8	6	4	8	8
6	6	8	6	6	6	6	8	10	6	8	8	6	6	6	8
6	8	6	6	4	10	6	6	6	6	6	6	6	8	6	6
6	8	8	6	8	6	6	6	6	6	6	10	6	6	8	6
8	6	8	10	8	8	8	6	6	8	6	10	6	6	8	6
6	8	6	6	8	6	6	6	12	6	6	8	6	6	6	6
8	6	6	6	8	6	6	8	8	6	6	8	6	6	6	6
8	8	6	8	6	6	8	8	8	6	6	8	8	8	8	6
6	8	6	6	6	6	8	6	6	6	6	6	6	6	8	6
6	6	6	8	8	8	8	6	6	6	8	6	10	8	8	8
6	6	8	8	8	6	6	12	6	4	6	6	8	8	6	–

Table 9 DP comparison

S-box	Max DP
Proposed	0.03125
[39]	0.03906
[24]	0.03906
[23]	0.03906

Discussion

The proposed S-box approach was evaluated in terms of NL, SAC, BIC, LP, and DP in which Table 11 displays the values of these terms for our S-box with other related S-boxes

Table 6 BIC–SAC criterion of our S-box

–	0.5087	0.4930	0.4908	0.4930	0.4840	0.5020	0.4885
0.5176	–	0.4885	0.5064	0.5176	0.5311	0.5064	0.5087
0.5199	0.5087	–	0.5087	0.5042	0.4975	0.5266	0.5020
0.5221	0.5132	0.5176	–	0.5154	0.5199	0.5468	0.5311
0.4952	0.4975	0.5221	0.4796	–	0.5020	0.4952	0.5020
0.5042	0.4997	0.5109	0.4952	0.5087	–	0.5042	0.5064
0.5087	0.5445	0.4997	0.4930	0.5176	0.4840	–	0.5333
0.5020	0.4952	0.5020	0.5109	0.4885	0.4997	0.4997	–

Table 10 Comparison of LP

S-box	LP
Proposed	0.1172
[39]	0.1172
[24]	0.1562
[23]	0.1250

reported in [6–8,23–26,29,30,34,39]. The S-boxes reported in [6,7,23–26] are based on chaotic systems, while the S-boxes reported in [8,29,30,39] are based on optimization algorithms to select a well-constructed S-box based on its performance analyses, not to utilize optimization algorithms in developing S-box mechanisms. The S-box reported in [34] is based on quantum-inspired QW, while the proposed S-box mechanism is based on quantum-inspired QW that can withstand possible assaults from both classical and quantum devices, and its structure is based on the customized PSO to provide extra security.

From the stated evaluations above, we can deduce that:

1. The proposed S-box mechanism is based on quantum-inspired QW and the customized PSO to provide extra security.
2. Table 1 proves the bijective characteristic of the constructed S-box.
3. Table 11 shows that the constructed S-box performs well in comparison to other S-boxes.
4. The average of the S-box's BIC–SAC value is 0.5030, which is extremely close to the ideal value.
5. The max value of DP, Table 9, is acceptable.
6. The LP value, Table 10, is acceptable.

Proposed encryption algorithm

Images are commonly utilized for representing the majority of data due to their having more detailed information. Using image encryption methods, digital images may be protected in which S-boxes are extensively utilized in the designing process of image cryptosystems. Due to the effectiveness of the proposed S-box algorithm, we propose a new image cryptosystem as a cryptographic purpose of this S-box algorithm. In the suggested image cryptosystem, the probability vector generated from operating quantum-inspired QW and the generated sequences from the Hénon map are utilized to operate the customized PSO algorithm for generating two sequences (X and Y), in which X and Y sequences are utilized for constructing different two permutation boxes to shuffle columns and rows of the pristine image. Then, the X sequence is utilized for constructing an 8 × 8 S-box to substitute the pixels of the permutated image, while the Y sequence is utilized for generating a pseudo-random sequence to generate the encrypted image from the substituted image. The framework of the suggested encryption algorithm is shown in Fig. 1, and the detailed steps of the encryption procedure are listed in the following points.

Step 1: Set the initial values of parameters (S, V, t, θ, σ_0, σ_1, σ_2, p_0, q_0, a, b,α, $d1$, $d2$, x_0, y_0).

Step 2: Acquire the hash code ($H = h_1, h_2, \ldots, h_{256}$) for the pristine image (PIm) using SHA-256 algorithm, and convert each 8-bit of H into integers ($N = n_1, n_2, \ldots, n_{32}$), then update the initial values of p_0, q_0, and S using N as stated in the following equations:

Table 11 Values of NL, SAC, BIC, LP, and DP for the constructed S-box compared with other related S-box algorithms

Algorithm	Technique	NL	BIC-NL	SAC	BIC-SAC	LP	DP
Proposed	Based on quantum-inspired QW and the customized PSO	107.00	103.0	0.5044	0.5066	0.1172	0.0313
[6] S-box1	Mackey–Glass equation	104.00	102.9	0.5000	0.4980	0.1328	0.0391
[6] S-box2	Mackey–Glass equation	104.00	102.7	0.4910	0.5005	0.1484	0.0468
[6] S-box3	Mackey–Glass equation	103.00	103.1	0.4990	0.4964	0.1328	0.0468
[25]	Based on Enhanced logistic map and Latin square	105.25	103.2	0.5351	0.5000	–	0.0391
[29]	Based on Jaya optimization algorithm	106.25	103.64	0.5009	0.4996	0.1171	0.0391
[23]	Based on a 3D chaotic map	106.00	104.2	0.4993	0.5030	0.1250	0.0391
[26]	Based on Gingerbreadman chaotic system	102.00	102.9	0.5178	0.4999	0.1250	0.0313
[24]	Based on logistic-sine map	105.25	103.8	0.4956	0.4996	0.1562	0.0391
[34]	Based on quantum-inspired QW	106.00	103.9	0.4958	0.5023	0.1250	0.0313
[7]	Based on a 3D chaotic map	106.50	103.1	0.5000	0.5058	0.1250	0.0391
[39]	Teaching-learning-based optimization	106.50	104.6	0.4995	0.4983	0.1172	0.0391
[30] Avg	Using parameter optimization of 1D chaotic systems	103.47	103.5	0.5008	0.5010	–	–
[8] Avg	Using improved PSO algorithm	104.11	103.4	0.5018	0.5017	0.1377	–

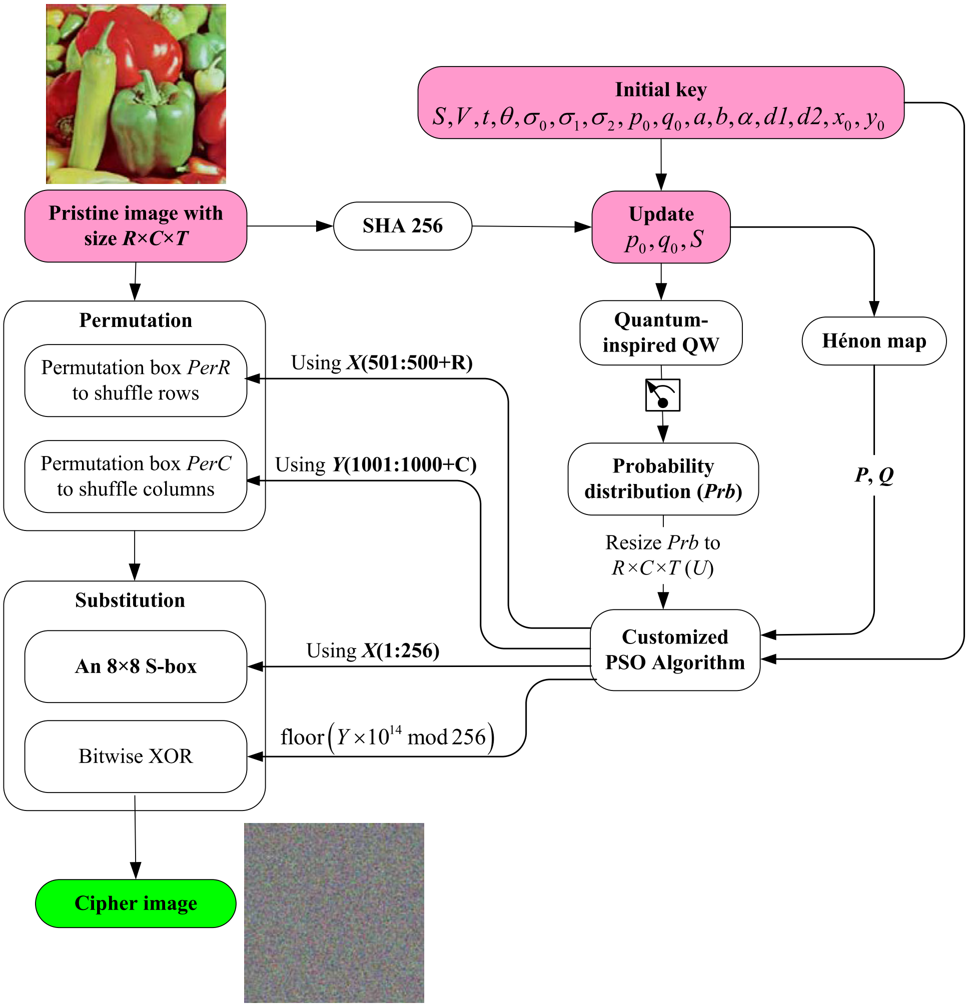

Initial key
$S, V, t, \theta, \sigma_0, \sigma_1, \sigma_2, p_0, q_0, a, b, \alpha, d1, d2, x_0, y_0$
Pristine image with size R×C×T
SHA 256
Update p_0, q_0, S
Quantum-inspired QW
Hénon map
Probability distribution (Prb)
P, Q
Resize Prb to R×C×T (U)
Permutation
Permutation box PerR to shuffle rows
Using X(501:500+R)
Permutation box PerC to shuffle columns
Using Y(1001:1000+C)
Substitution
An 8×8 S-box
Using X(1:256)
Customized PSO Algorithm
Bitwise XOR
floor($Y \times 10^{14}$ mod 256)
Cipher image

Fig. 1 Description of the offered encryption scheme

$$p_{\text{new}} = \left(p_0 + \frac{n_1 \oplus n_2 \oplus \cdots \oplus n_8}{256}\right)/2, \tag{12}$$

$$q_{\text{new}} = \left(q_0 + \frac{n_9 \oplus n_{10} \oplus \cdots \oplus n_{16}}{256}\right)/2, \tag{13}$$

$$S_{\text{new}} = \left[\, S \text{ de2bi}\left(\textstyle\sum_{k=17}^{32} n_k\right) \right]. \tag{14}$$

Step 3: Using $S_{\text{new}}, V, t, \theta, \sigma_0, \sigma_1, \sigma_2$ operate QW for t steps on a circle of V-vertex, for producing a probability vector Prb of length V, then resize the elements of the Prb vector to another vector of length $R \times C \times T$, where $R \times C$ is the size of the original image PIm and T is the number of color components in PIm

$$U = \text{resize}\left(\text{Prb}, \left[\, RCT \;\; 1 \,\right]\right). \tag{15}$$

Step 4: Using p_{new}, q_{new}, a, b iterate Hénon map for g times, and generating two chaotic sequences (P, Q) each of length $R \times C \times T$, then from theses sequences generate three sequences as given below

$$V = P \mod 1, \tag{16}$$

$$Z = Q \mod 1, \tag{17}$$

$$W = (P - Q) \mod 1. \tag{18}$$

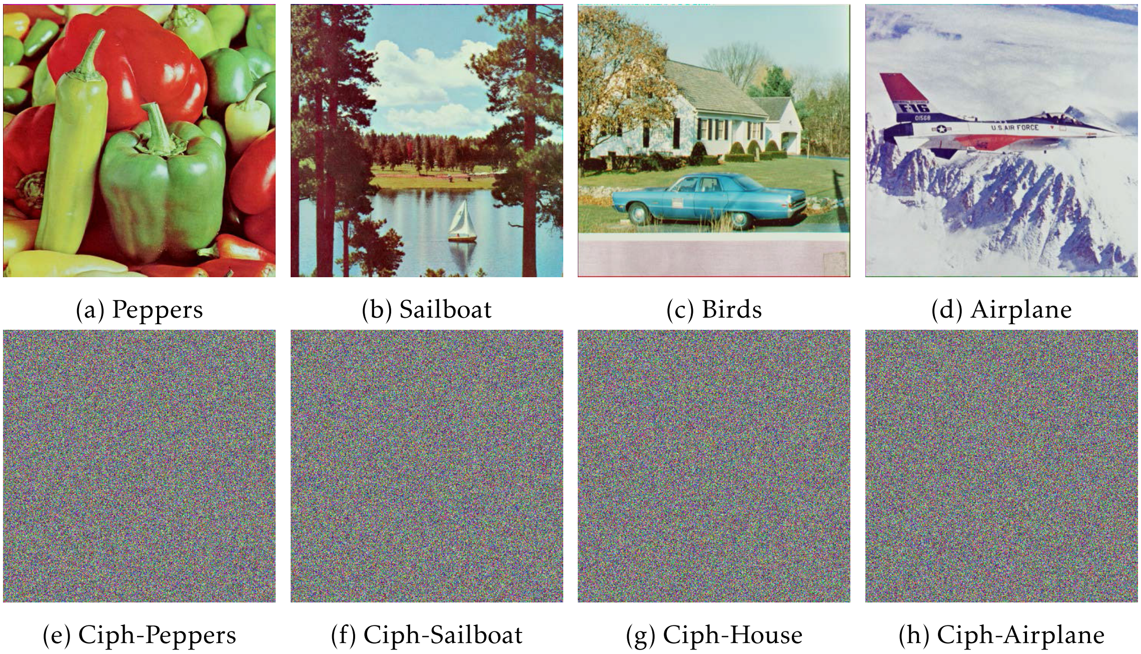
Step 5: Using parameters (α, $d1$, $d2$, x_0, y_0) and the generated sequences (U, V, Z, W) operate the customized PSO (7) for generating two sequences (X, Y) each of length $R \times C \times T$.

Step 6: Constructing a permutation box to shuffle rows of PIm image by arranging the elements of a sequence A (where $A = X(501{:}500 + R)$) in ascending order as a sequence B, then locate the index of per element of B in A as permutation box PerR.

Step 7: Similar to constructing PerR, construct PerC using sequence $Y(1001{:}1000 + C)$ to shuffle columns.

Step 8: Permutate the pristine image PIm using the constructed permutation boxes PerR and PerC

$$\text{PerIm}\,(i, j, :) = \text{PIm}\,(\text{PerR}(i), \text{PerC}(j), :)$$
$$\text{for } i = 1 \text{ to } R,\;\; j = 1 \text{ to } C.$$



(a) Peppers (b) Sailboat (c) Birds (d) Airplane

(e) Ciph-Peppers (f) Ciph-Sailboat (g) Ciph-House (h) Ciph-Airplane

Fig. 2 Utilized dataset and its cipher images using the suggested cryptosystem

Step 9: Construct an 8 × 8 S-box (Sb) using sequence $X(1{:}256)$, and substitute the permutated image PerIm using Sb

$$\text{SubIm}\,(i,\,j,k) = \text{Sb}\,(\text{PerIm}(i,\,j,k))$$
$$\text{for } i = 1 \text{ to } R,\;\; j = 1 \text{ to } C,\;\; k = 1 \text{ to } T.$$

Step 10: To construct the final cipher image (CiphIm), convert the Y sequence to integer values (K) and use K to perform the BitXor operation with the substituted image SubIm

$$K = \text{floor}\left(Y \times 10^{14} \mod 256\right), \tag{19}$$
$$\text{CiphIm} = K \oplus \text{SubIm}. \tag{20}$$

Experimental outcomes and analyses

To appreciate the competence of the suggested image cryptosystem, we utilized a dataset of color images brought from SIPI image database [40], in which the dimension of each image is 512 × 512. Experiments were carried out using the MATLAB software version R2016b, which was installed on a PC with an Intel Core$^{\text{TM}}$ Due 3 GHz processor and 4GB of RAM. The initial key parameters are set as: S = [0100 0100 1011 1101 0101 0101 0110 1001 1010 0110 0101], $V = 265$, $t = 271$, $\theta = 0$, $\sigma_0 = \pi/3$, $\sigma_1 = \pi/4$, $\sigma_2 = \pi/6$, $p_0 = 0.6495$, $q_0 = 0.5073$, $a = 1.4$, $b = 0.3$, $\alpha = 0.1$, $d1 = 0.5$, $d2 = 0.5$, $x_0 = 0.5$, and $y_0 = 1$.

The cipher images for the supplied dataset are shown in Fig. 2, in which no visual information about pristine images can be gained from encrypted images. In addition to visual effects, several analyses were carried out to validate the effectiveness of the proposed cryptosystem.

Complexity analysis

To check the efficacy of the suggested encryption scheme in terms of computational cost, we examine it from two viewpoints: computational complexity and encryption time.

The presented encryption approach primarily includes three phases: key generation, confusion, and diffusion. The utilized key streams are generated using Hénon map, QW, and the customized PSO. Hénon map iterates RC times, where RC is the dimensions of the original image, therefore the complexity of operating Hénon map is thus $\mathcal{O}(RC)$; and the complexity of acting QW on a cycle of V-vertex is $\mathcal{O}(V^2)$, while the complexity of operating the customized PSO (7) is $\mathcal{O}(RC)$. The confusion strategy is based on two permutation boxes, one for acting rows and the other for acting columns which both are based on sorting the elements and locating the index of per element, with an $\mathcal{O}(\max(R \log R, C \log C))$ computational complexity. The diffusion strategy is based on constructing an S-box with an $\mathcal{O}(256 \log 256)$ computational complexity, and the bitwise XOR operation with an $\mathcal{O}(RC)$. According to the reported computational complexity for each component of the suggested encryption approach, the whole computational complexity of the encryption approach is $\mathcal{O}(\max(RC, V^2))$.

Table 12 Comparison of the recommended scheme's encryption time in megabytes/second to that of other relevant techniques

Algorithm	Data encrypted (in megabytes/s)
Proposed	0.669703
[15]	0.592556
[20]	0.477463
[18]	0.403226
[7]	0.271800
[23]	0.209639
[24]	0.163086
[41]	0.035047
[29]	0.025580
[10]	0.004096

Encryption time is known as the time taken to cipher one image. Table 12 provided a quick comparison of the recommended scheme's encryption time in megabytes/second to that of other relevant techniques as reported in [7,10,15,18,20,23,24,29,41]. Based on the data displayed in Table 12, the presented encryption technique has an admissible time complexity and broad applicability.

Note that the constructed S-box using our methodology is generated once, not several times as in other S-box mechanisms that are based on optimization algorithms. Also, the cipher image is constructed once, not several times as in other image cryptosystems that are based on optimization algorithms. Therefore, our methodology has better performance and usability than other related methodologies that are based on optimization algorithms.

Correlation analysis

The correlation coefficient (Crf) of adjoining pixels is utilized to appreciate the meaning of an image, in which pristine images have strong Crf values close to 1 and good cipher images have Crf values close to 0. To calculate the Crf values for our experimented dataset and its related cipher images, we randomly selected 10^4 pairs of adjacent pixels. Crf can be stated mathematically as follows

$$\mathrm{Crf} = \frac{\sum_{j=1}^{M}\left(x_j - \bar{x}\right)\left(y_j - \bar{y}\right)}{\sqrt{\sum_{j=1}^{M}\left(x_j - \bar{x}\right)^2 \sum_{j=1}^{M}\left(y_j - \bar{y}\right)^2}}, \tag{21}$$

where M represents the number of adjacent pixel pairs x_j and y_j. Table 13 states the Crf values for the investigated dataset, in which the Crf values for cipher images are very near to 0. To support Table 13 visually, Figs. 3, 4, and 5 plot the correlation distribution for Peppers image before and after the encryption procedure. From the stated outcomes in this subsection, we can extrapolate that the proposed cryptosystem is secure against correlation analysis.

Differential analysis

Differential analysis is utilized to appreciate the number of differences between two encrypted images for one plain image with slight modifications in one bit. There are two measures that are utilized in differential analyses: NPCR ("Number of Pixel Change Rate") and UACI ("Unified Average Changing Intensity"), which are stated as given below

$$\begin{aligned} \mathrm{NPCR} &= \frac{\sum_{a;b} f(a,b)}{M} \times 100\% \quad , \\ f(a,b) &= \begin{cases} 0 & \text{if } R1(a,b) = R2(a,b) \\ 1 & \text{if } R1(a,b) \neq R2(a,b) \end{cases} \end{aligned} \tag{22}$$

$$\mathrm{UACI} = \frac{1}{M}\left(\sum_{a,b} \frac{|R1(a,b) - R2(a,b)|}{255}\right) \times 100\%, \tag{23}$$

where M signifies the complete number of pixels in the image and $R1$, $R2$ represent two encrypted images for one plain image with slight modifications in one bit. The results of

Table 13 Crf outcomes for the investigated dataset

Image	Direction								
	Hori.			Vert.			Diag.		
	R	G	B	R	G	B	R	G	B
Peppers	0.9679	0.9833	0.9702	0.9658	0.9834	0.9656	0.9594	0.9718	0.9508
Ciph-Peppers	0.0007	0.0009	0.0005	– 0.0008	– 0.0003	0.0004	– 0.0009	– 0.0005	0.0004
Sailboat	0.9576	0.9671	0.9683	0.9584	0.9722	0.9714	0.9476	0.9538	0.9516
Ciph-Sailboat	0.0011	– 0.0002	– 0.0007	– 0.0002	– 0.0012	– 0.0008	0.0004	0.0006	– 0.0009
House	0.9585	0.9477	0.9728	0.9604	0.9412	0.9713	0.9262	0.8989	0.9468
Ciph-House	– 0.0001	– 0.0006	– 0.0002	0.0001	– 0.0007	0.0003	– 0.0003	0.0001	– 0.00008
Airplane	0.9649	0.9681	0.9400	0.9715	0.9690	0.9653	0.9416	0.9439	0.9202
Ciph-Airplane	0.0001	0.0003	0.0001	0.0002	– 0.0003	– 0.0004	– 0.0003	0.0008	0.0001

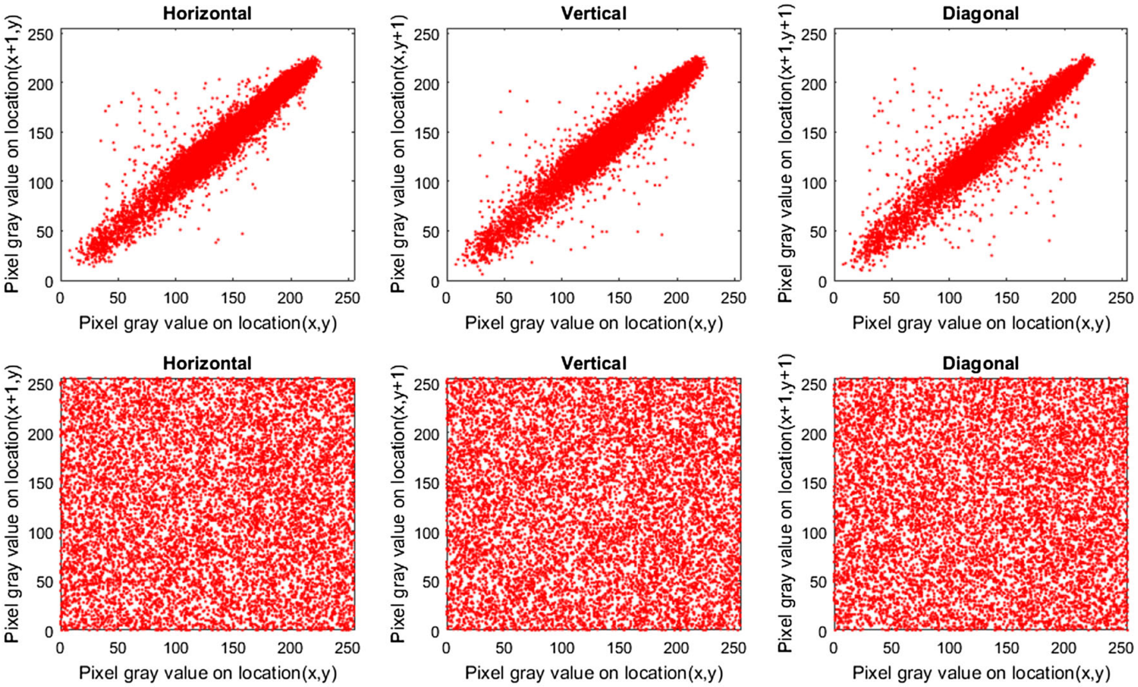


Fig. 3 The correlation distribution for Peppers image (red channel), in which the first row represents the original image, while the second row is for the cipher image

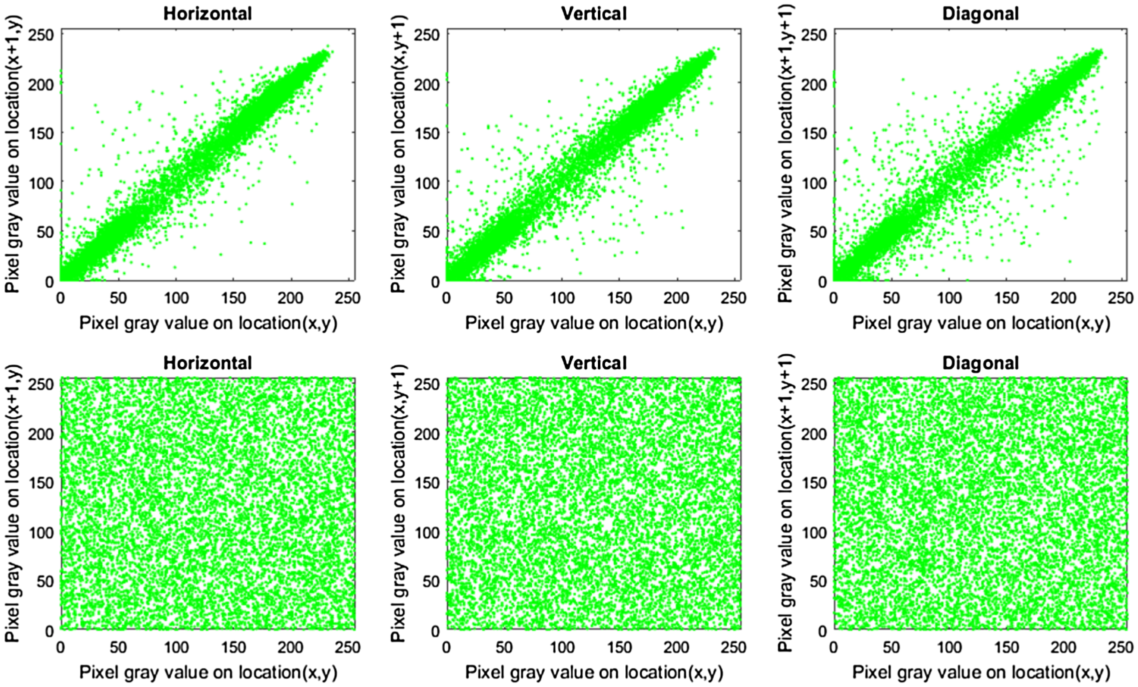


Fig. 4 The correlation distribution for Peppers image (green channel), in which the first row represents the original image, while the second row is for the cipher image

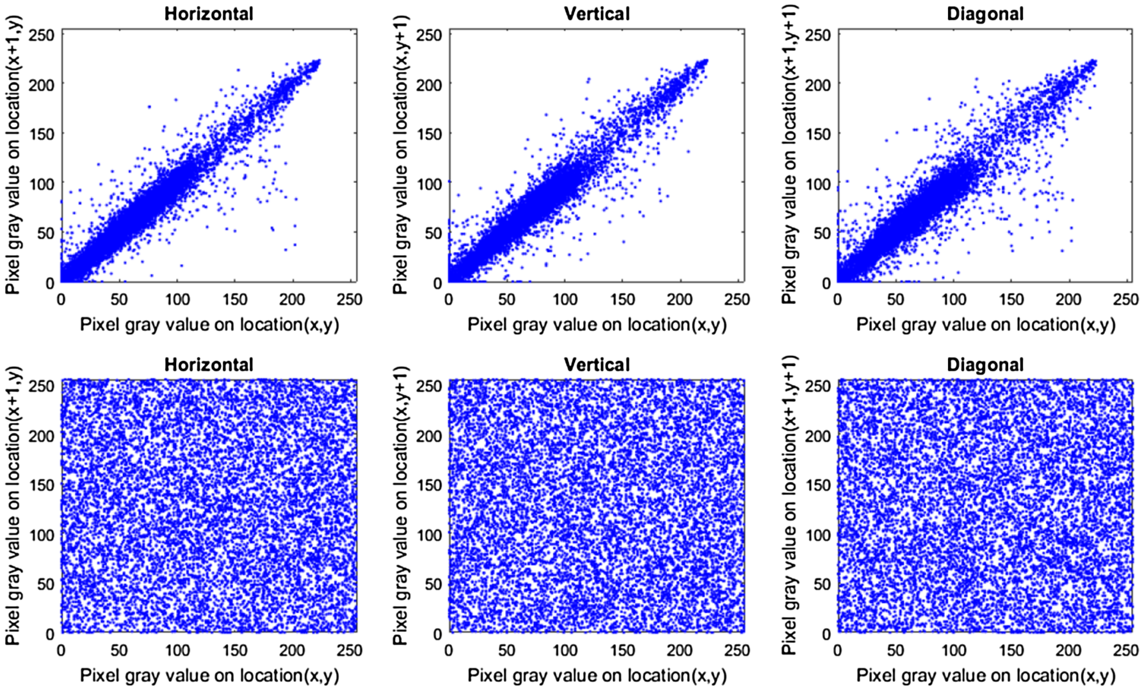


Fig. 5 The correlation distribution for Peppers image (blue channel), in which the first row represents the original image, while the second row is for the cipher image

Table 14 UACI and NPCR results

Image	UACI%	NPCR%
Peppers	33.4855	99.6121
Sailboat	33.4838	99.6209
House	33.4931	99.6239
Airplane	33.4744	99.6159

NPCR and UACI are given in Table 14, in which NPCR values for all cipher images exceed 99.60% and UACI values are around 33.46%. Therefore, the suggested encryption algorithm has high pristine image sensitivity.

Key sensitivity analysis

Key sensitivity analysis is utilized to appreciate the decryption effects of cipher images with slight modifications in initial key parameters. Figure 6 displays the visual effects of deciphering the Ciph-Peppers image with slight modifications in initial key parameters, from which we can deduce that the presented encryption technique has high key sensitivity.

Histogram analysis

A histogram is used to appreciate the distribution of pixel values in an image. Cipher images generated by a well-developed cryptosystem should have indistinguishable histograms for different encrypted images. Figure 7 shows the histograms of the experimented dataset and its resulting encrypted images, in which the plots for the encrypted images are semi-similar to each other. To verify that the constructed cipher images have a regular distribution of histograms, we utilized a numerical test like the Chi-square (χ^2) test whose mathematical expression is given below

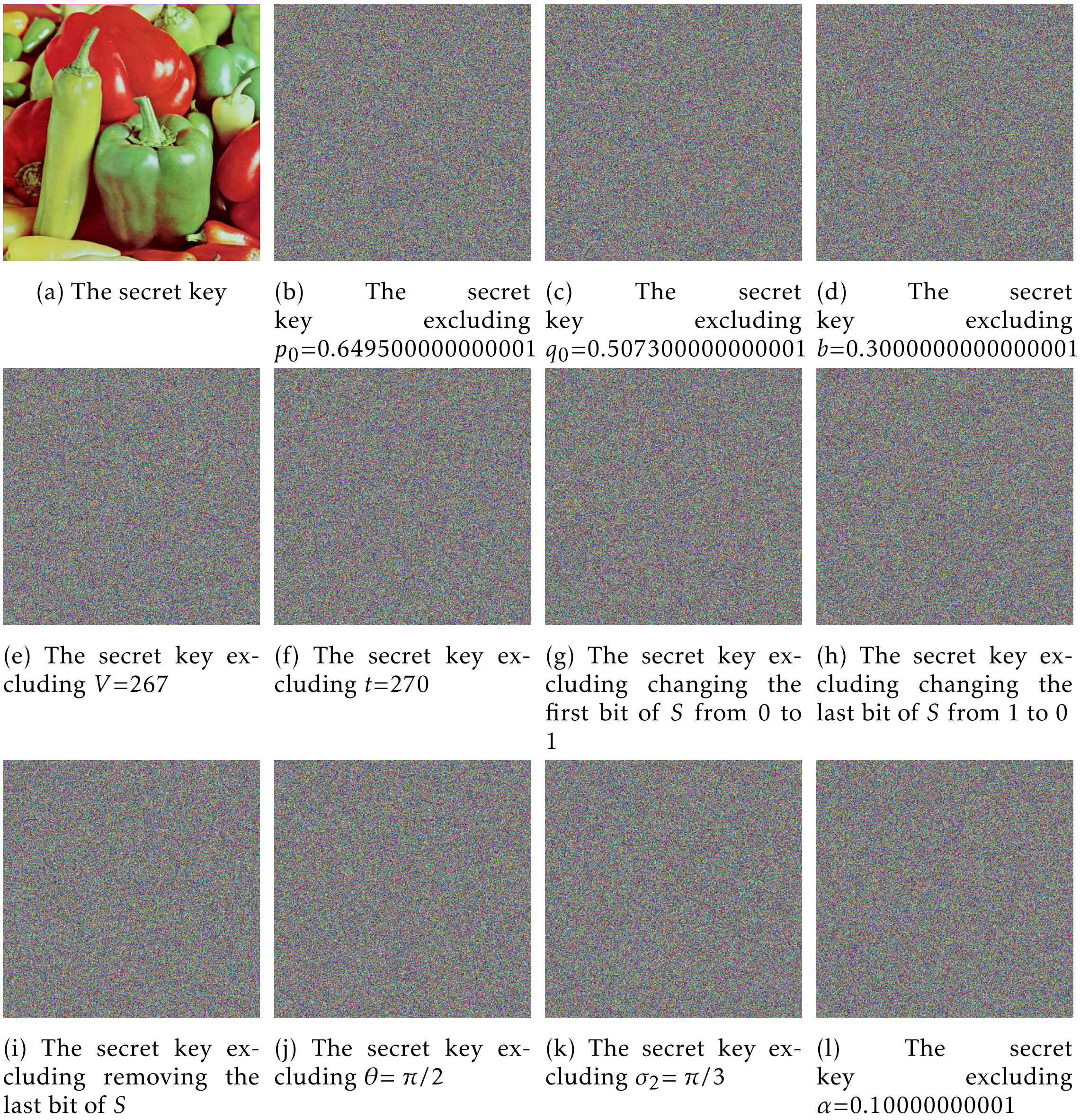
$$\chi^2 = \sum_{i=0}^{255} \frac{(r_i - s)^2}{s}, \tag{24}$$

where r_i is the frequency of the pixel value i, and s represents the dimension of the image. If the χ^2 value does not exceed the threshold value $\chi^2_{0.05}(255) = 293.3$, then its histogram is regular, else the image has a non-uniform histogram. The outcomes of χ^2 are given in Table 15, in which the χ^2 values for all encrypted images are less than 293.3. Therefore, the suggested image cryptosystem can withstand histogram analysis attacks.

Entropy analysis

Image entropy test is used to appreciate the distribution of bit levels in an image. Cipher images constructed by a well-developed image encryption should have an entropy value very close to 8. The mathematical expression for entropy is given in Eq. (25)

$$E(A) = -\sum_{i=0}^{255} r(a_i) \log_2 (r(a_i)), \tag{25}$$



(a) The secret key

(b) The secret key excluding p_0=0.6495000000000001

(c) The secret key excluding q_0=0.5073000000000001

(d) The secret key excluding b=0.3000000000000001

(e) The secret key excluding V=267

(f) The secret key excluding t=270

(g) The secret key excluding changing the first bit of S from 0 to 1

(h) The secret key excluding changing the last bit of S from 1 to 0

(i) The secret key excluding removing the last bit of S

(j) The secret key excluding $\theta = \pi/2$

(k) The secret key excluding $\sigma_2 = \pi/3$

(l) The secret key excluding α=0.10000000001

Fig. 6 Visual effects of deciphering the Ciph-Peppers image with slight modifications in initial key parameters

where $r(a_i)$ represents the probability of a_i. Table 16 states the results of the entropy test, in which cipher images have entropy values very approximately 8-bit. Hence, the suggested encryption approach can resist entropy attacks.

Occlusion analysis

To appreciate the suggested encryption scheme against occlusion attacks, we made cuts out of some parts of the encrypted image and then tried to decipher it. Figure 8 shows the outcomes of occlusion attacks, in which the deciphered image is recovered perfectly without lack of any visual information in the cutout part.

Classical attacks

Generally, the cryptanalyst is familiar with the design and the operation of the under-consideration cryptosystem, aware of virtually everything about the encryption algorithm except the key parameters. A well-developed encryption algorithm must be has the ability to resist common attacks such as known-plaintext, ciphertext-only, chosen-ciphertext, and chosen-plaintext attacks. A cryptoanalyst in ciphertext-only attacks has only the ciphertext he has trapped, but in known-plaintext attacks, the cryptoanalyst has pairs of plaintext–ciphertext and tries to breach the secret key. In chosen-plaintext attacks, the cryptoanalyst has the ciphertext for a selected plaintext by himself, whereas in chosen-

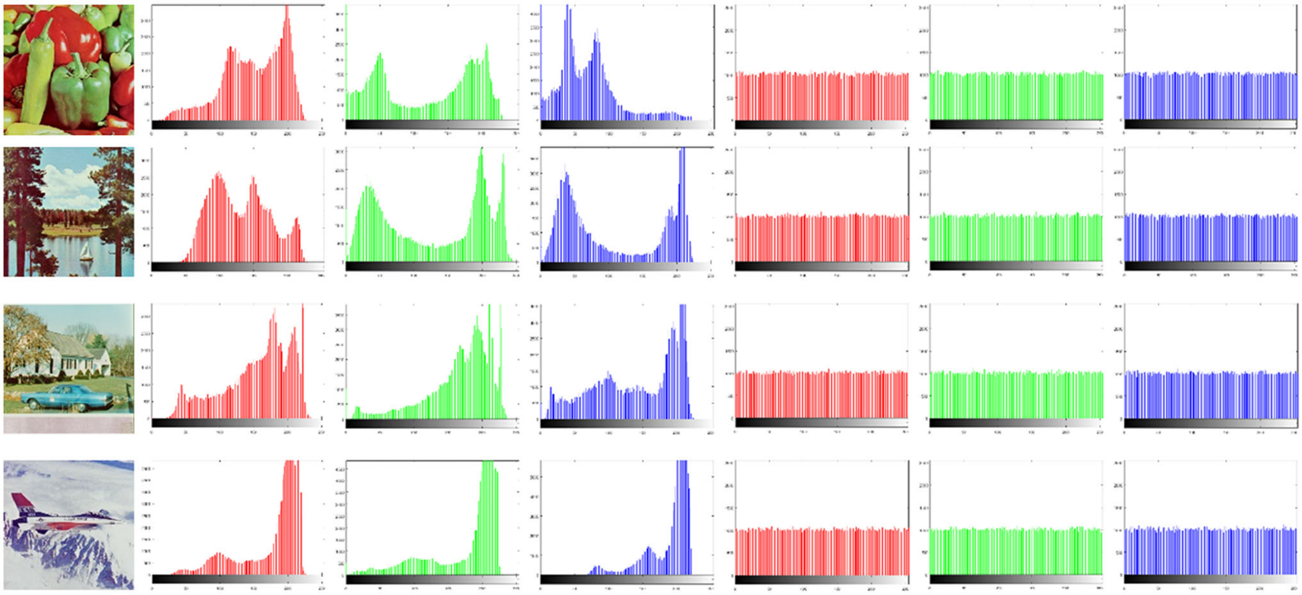


Fig. 7 Histograms of the investigated dataset and its resulting cipher images, in which the last three columns are devoted to cipher images, while other histograms are for the pristine images

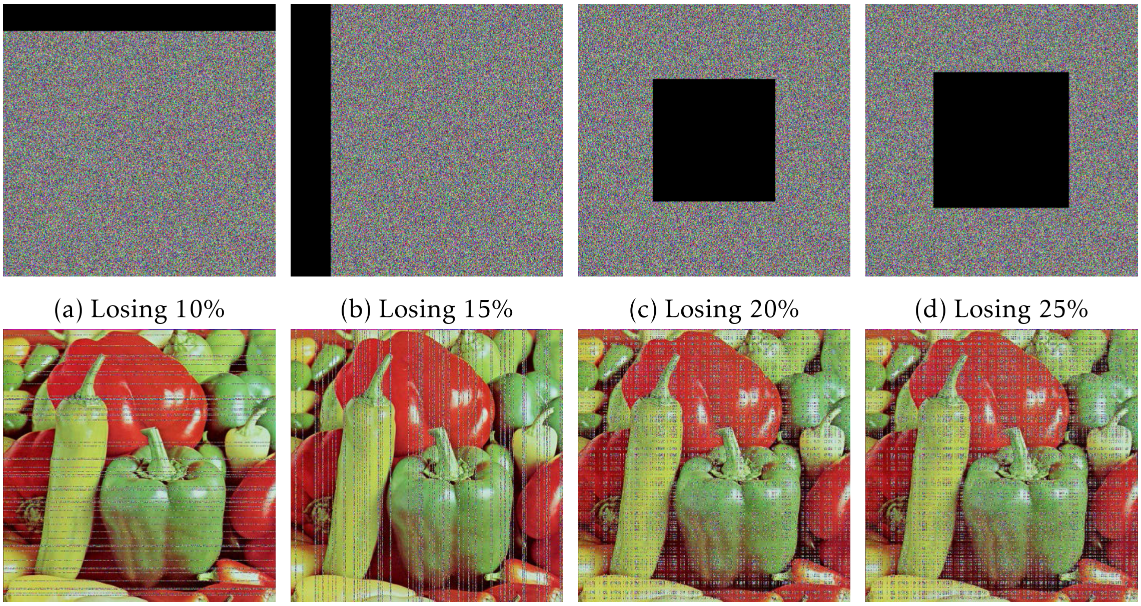
Table 15 The outcomes of χ^2 test

Image	χ^2 values for each color component			Result
	R	*G*	*B*	
Peppers	21,3187.2167	318,382.9296	491,428.1777	Distinguishable
Sailboat	196,697.3066	130,154.7167	344,571.5371	Distinguishable
House	192,029.6504	332,540.1172	248,006.8476	Distinguishable
Airplane	678,424.4921	682,495.3828	1,107,858.0058	Distinguishable
Ciph-Peppers	245.8105	223.9609	247.4980	Indistinguishable
Ciph-Sailboat	252.4707	274.8359	228.2363	Indistinguishable
Ciph-House	263.7128	240.4414	248.5957	Indistinguishable
Ciph-Airplane	263.4355	240.5722	264.1992	Indistinguishable

Table 16 Entropy results

Image	Plain	Cipher
Peppers	7.669825	7.999803
Sailboat	7.762169	7.999765
House	7.485787	7.999767
Airplane	6.663908	7.999746

ciphertext attacks, the cryptoanalyst has the plaintext for a chosen ciphertext. The chosen-plaintext attack is the most powerful known assault, in which the cryptoanalyst earns transitory access to the cryptosystem and constructs ciphertext associated with a picked plaintext, attempting to breach the secret key or devising a strategy to decipher the ciphertext even access to the secret key. If an encryption approach can endure the chosen-plaintext attack, it can also endure other types of assaults. Due to the fact that the used keystream in the encryption procedure for our cryptosystem is based on the pristine image, the cryptoanalyst for the suggested encryption algorithm cannot get any information about the original key parameters by examining the ciphertext. In another manner, for each pristine image, a one-time keystream is generated, while the original key parameters remain unmodified. Because the totally paralyzed responsibilities of permutation and substitution procedures, cryptoanalysts prefer to nominate full-back and full-white images in chosen-plaintext assaults. The cipher images for FullBlack and FullWhite images, as well as their related histograms, are shown in Fig. 9, where no visual information can be acquired, and some statistical analyses for those images are stated in Table 17. As a consequence, the presented cryptosystem can withstand classical attacks.



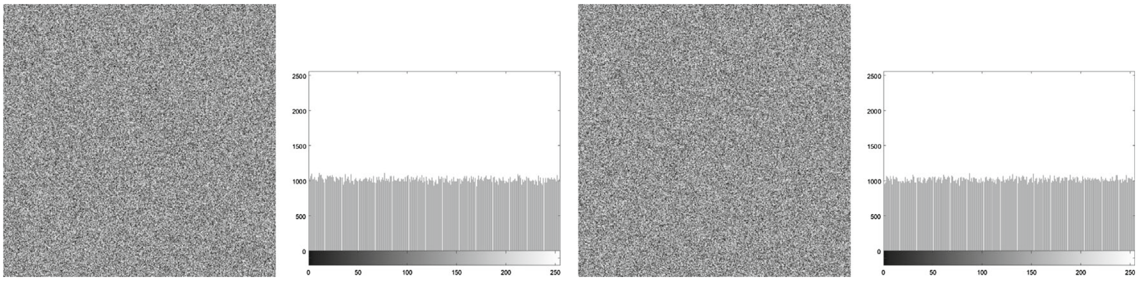
(a) Losing 10%

(b) Losing 15%

(c) Losing 20%

(d) Losing 25%

Fig. 8 Occlusion outcomes



(a) Ciph-FullWhite

(b) Histogram of (a)

(c) Ciph-FullBlack

(d) Histogram of (c)

Fig. 9 Cipher images for FullBlack and FullWhite images and their histograms

Table 17 Statistical analyses of Ciph-FullWhite and Ciph-FullBlack images

Image	χ^2 value	Entropy	Correlation		
			Hori.	Vert.	Diag
Ciph-FullWhite	271.4629	7.999142	0.0011	0.0005	– 0.0003
Ciph-FullBlack	257.5254	7.999291	0.0008	0.0005	– 0.0005

Discussion

The presented encryption approach was evaluated from two viewpoints to prove its effectiveness: performance and withstanding cryptanalysis attacks. Regarding performance, the final cipher image is constructed once, not several times as in other image cryptosystems that are based on optimization algorithms; and based on the data displayed in Table 12, the presented encryption technique has an admissible time complexity and broad applicability. Therefore, our methodology has better performance and usability than other related methodologies that are based on optimization algorithms.

Regarding cryptanalysis attacks, we performed several analyses to evaluate the presented encryption approach for withstanding differential, statistical, occlusion, brute-force, and classical types of attacks. Table 13 states the correlation coefficients for the analyzed dataset, in which its values for cipher images are very near to 0. To support Table 13 visually, Figs. 3, 4, and 5 plot the correlation distribution for Peppers image before and after the encryption procedure. Cipher images constructed by a well-designed cryptosystem should have indistinguishable histograms for different cipher images. Figure 7 displays the histograms of the investigated dataset and its resulting encrypted images, in which

Table 18 Comparison of the suggested encryption technique with other corresponding ones

Technique	UACI (%)	NPCR (%)	Chi-square	Entropy	Correlation		
					Diag.	Vert.	Hori.
Proposed	33.484	99.618	249.481	7.99977	– 0.00004	– 0.00031	0.00015
[3]	33.380	99.615	–	7.99715	0.00340	– 0.00085	– 0.00025
[4]	33.843	99.692	–	7.99910	0.00460	0.00210	0.00120
[5]	33.117	99.627	–	7.99358	0.00111	– 0.00032	0.00168
[23]	33.470	99.608	–	7.99984	– 0.00014	0.00007	0.00007
[21]	33.483	99.613	254.431	7.99984	0.00012	– 0.00002	0.00018
[18]	33.473	99.600	264.417	7.99930	– 0.00034	0.00083	– 0.00063
[20]	33.427	99.607	256.752	7.99866	– 0.00250	0.00170	0.00050
[41]	33.440	99.600	257.337	7.99700	0.00650	– 0.00870	– 0.00970

the plots for the encrypted images are semi-similar to each other. To verify that the constructed cipher images have a regular distribution of histograms, χ^2-test is utilized. The results of χ^2 are provided in Table 15, in which the χ^2 values for all cipher images are < 293.3. Cipher images constructed by a well-developed cryptosystem should have an entropy value very close to 8. Table 16 states the results of the entropy test, in which cipher images have entropy values of very approximately 8 bits. From the results of correlation, histogram, and entropy analyses, we can extrapolate that the proposed cryptosystem is secure against statistical analysis. Differential analysis is utilized to appreciate the number of differences between two encrypted images for one plain image with slight modifications in one bit. There are two measures that are utilized in differential analyses: NPCR and UACI. The results of NPCR and UACI are given in Table 14, in which NPCR values for all cipher images are $> 99.60\%$ and UACI values are around 33.46%. Therefore, the suggested encryption algorithm has high pristine image sensitivity. Figure 6. displays the visual effects of deciphering the Ciph-Peppers image with slight modifications in initial key parameters, from which we can deduce that the presented encryption technique has high key sensitivity. To appreciate the suggested encryption scheme against occlusion attacks, we made cuts out of some parts of the cipher image and then tried to decipher it. Figure 8 shows the results of occlusion attacks, in which the ciphered image is restored perfectly without lack of any visual information in the cutout part. If an encryption approach can resist the chosen-plaintext attack, it can also resist other types of assaults. Due to the fact that the used keystream in the encryption procedure for our cryptosystem is based on the pristine image, the cryptoanalyst for the suggested encryption algorithm cannot gain any information about the original key parameters by examining the ciphertext. The ciphered images for FullBlack and FullWhite images, as well as their related histograms, are shown in Fig. 9, where no visual information can be acquired, and some statistical analyses for those images are stated in Table 17. As a consequence, the proposed cryptosystem can resist classical attacks. To verify the effectiveness of the offered encryption scheme alongside other corresponding ones, Table 18 stated the average values of UACI, NPCR, Chi-square, entropy, and correlation coefficients for the suggested scheme and their values in other corresponding ones. From the given values in Table 18, we deduce that the suggested encryption algorithm is effective and has high security.

Conclusion

The key contribution of this study is to pave the way to utilizing quantum-inspired models with optimization algorithms in designing robust S-boxes. In this paper, a new S-box technique based on quantum-inspired QW, Hénon map, and the customized PSO algorithm is proposed. Several analyses were performed to assess the effectiveness of the presented S-box technique, and its outcomes were utterly acceptable. Also, a new image cryptosystem based on the presented S-box approach is proposed. The stated experimental outcomes for the suggested cryptosystem prove its effectiveness and the reliability of the suggested S-box approach for various cryptographic purposes.

But the proposed cryptosystem is only appropriate for transmitting images securely over communication channels; it is not appropriate for other data types, such as text, video, audio, etc. This is one of the study's drawbacks. Future modifications to the proposed technique will be made to support the secure transmission of diverse data types over communication channels.

Acknowledgements The author gratefully acknowledges the unconditional support of his family.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

Data availability statement The data used in the study can be accessed upon your request to the corresponding author.

Declarations

Conflict of interest The author declares that he has no conflict of interest.

Ethics approval This research contains neither human nor animal studies.

References

1. Uddin M, Jahan F, Islam MK, Hassan MR (2021) A novel DNA-based key scrambling technique for image encryption. Complex Intell Syst 7:3241–3258
2. Gan Z, Chai X, Bi J, Chen X (2022) Content-adaptive image compression and encryption via optimized compressive sensing with double random phase encoding driven by chaos. Complex Intell Syst 8:2291–2309
3. Maazouz M, Toubal A, Bengherbia B, Houhou O, Batel N (2022) FPGA implementation of a chaos-based image encryption algorithm. J King Saud Univ Comput Inf Sci 34(10):9926–9941
4. Naseer Y, Shah T, Shah D (2021) A novel hybrid permutation substitution base colored image encryption scheme for multimedia data. J Inf Secur Appl 59:102829
5. Roy S, Shrivastava M, Rawat U, Pandey CV, Nayak SK (2021) IESCA: an efficient image encryption scheme using 2-d cellular automata. J Inf Secur Appl 61:102919
6. Khan NA, Altaf M, Khan FA (2020) Selective encryption of JPEG images with chaotic based novel s-box. Multimedia Tools Appl 80:9639–9656
7. El-Latif AAA, Ramadoss J, Abd-El-Atty B, Khalifa HS, Nazarimehr F (2022) A novel chaos-based cryptography algorithm and its performance analysis. Mathematics 10:2434
8. Hematpour N, Ahadpour S (2020) Execution examination of chaotic s-box dependent on improved PSO algorithm. Neural Comput Appl 33:5111–5133
9. Zamli KZ (2021) Optimizing s-box generation based on the adaptive agent heroes and cowards algorithm. Expert Syst Appl 182:115305
10. Saravanan S, Sivabalakrishnan M (2021) A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption. Soft Comput 25:5299–5322
11. Noshadian S, Ebrahimzade A, Kazemitabar SJ (2018) Optimizing chaos based image encryption. Multimedia Tools Appl 77:25569–25590
12. Poli R, Kennedy J, Blackwell T (2007) Particle swarm optimization. Swarm Intell 1:33–57
13. Karaboga D, Basturk B (2008) On the performance of artificial bee colony (ABC) algorithm. Appl Soft Comput 8:687–697
14. Dorigo M, Birattari M, Stutzle T (2006) Ant colony optimization. IEEE Comput Intell Mag 1:28–39
15. Luo Y, Ouyang X, Liu J, Cao L, Zou Y (2022) An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system. Soft Comput 26:5409–5435
16. Abd-El-Atty B, ElAffendi M, El-Latif AAA (2022) A novel image cryptosystem using gray code, quantum walks, and Henon map for cloud applications. Complex Intell Syst
17. Jiang N, Dong X, Hu H, Ji Z, Zhang W (2019) Quantum image encryption based on Henon mapping. Int J Theor Phys 58:979–991
18. Wang X, Gao S (2020) Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inf Sci 539:195–214
19. Rupa C, Harshita M, Srivastava G, Gadekallu TR, Maddikunta PKR (2022) Securing multimedia using a deep learning based chaotic logistic map. IEEE J Biomed Health Inform, p 1
20. Askar S, Karawia A, Al-Khedhairi A, Al-Ammar F (2019) An algorithm of image encryption using logistic and two-dimensional chaotic economic maps. Entropy 21:44
21. S. Vaidyanathan, A. Sambas, E. Tlelo-Cuautle, A. A. A. El-Latif, B. Abd-El-Atty, O. Guillen-Fernandez, K. Benkouider, M. A. Mohamed, M. Mamat, and M. A. H. Ibrahim, "A new 4-d multistable hyperchaotic system with no balance point: Bifurcation analysis, circuit simulation, FPGA realization and image cryptosystem," IEEE Access, vol. 9, pp. 144555–144573, (2021)
22. Rehman MU, Shafique A, Ghadi YY, Boulila W, Jan SU, Gadekallu TR, Driss M, Ahmad J (2022) A novel chaos-based privacy-preserving deep learning model for cancer diagnosis. IEEE Trans Netw Sci Eng 9(6):4322–4337
23. El-Latif AAA, Abd-El-Atty B, Belazi A, Iliyasu AM (2021) Efficient chaos-based substitution-box and its application to image encryption. Electronics 10:1392
24. Belazi A, Khan M, El-Latif AAA, Belghith S (2016) Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption. Nonlinear Dyn 87:337–361
25. Hua Z, Li J, Chen Y, Yi S (2021) Design and application of an s-box using complete Latin square. Nonlinear Dyn 104:807–825
26. Khan M, Asghar Z (2016) A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and s8 permutation. Neural Comput Appl 29:993–999
27. Zamli KZ, Kader A, Din F, Alhadawi HS (2021) Selective chaotic maps Tiki-Taka algorithm for the s-box generation and optimization. Neural Comput Appl 33:16641–16658
28. Alhadawi HS, Majid MA, Lambić D, Ahmad M (2020) A novel method of s-box design based on discrete chaotic maps and cuckoo search algorithm. Multimedia Tools Appl 80:7333–7350
29. Farah MAB, Farah A, Farah T (2019) An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dyn 99:3041–3064
30. E. Tanyildizi and F. Ozkaynak, "A new chaotic s-box generation method using parameter optimization of one dimensional chaotic maps," IEEE Access, vol. 7, pp. 117829–117838, (2019)
31. Wang X, Li Y (2021) Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Opt Lasers Eng 137:106393
32. Zeng J, Wang C (2021) A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata. Secur Commun Netw 2021:1–15
33. Ahmad M, Alam MZ, Umayya Z, Khan S, Ahmad F (2018) An image encryption approach using particle swarm optimization and chaotic map. Int J Inf Technol 10:247–255

34. El-Latif AAA, Abd-El-Atty B, Amin M, Iliyasu AM (2020) Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. Sci Rep 10:1930
35. Abd-El-Atty B (2023) A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. Neural Comput Appl 35:773–785
36. Venegas-Andraca SE (2012) Quantum walks: a comprehensive review. Quantum Inf Process 11:1015–1106
37. Li Z, He Y (2018) Steganography with pixel-value differencing and modulus function based on PSO. J Inf Secur Appl 43:47–52
38. A. Belazi and A. A. A. El-Latif, "A simple yet efficient s-box method based on chaotic sine map," Optik, 130, 1438–1444, (2017)
39. Farah T, Rhouma R, Belghith S (2016) A novel method for designing s-box based on chaotic map and teaching-learning-based optimization. Nonlinear Dynamics 88:1059–1074
40. Sipi image database-misc. http://sipi.usc.edu/database/database.php?volume=misc. Accessed 18 July 2022
41. Gan ZH, Chai XL, Han DJ, Chen YR (2018) A chaotic image encryption algorithm based on 3-d bit-plane permutation. Neural Comput Appl 31:7111–7130

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