IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 May 2023, accepted 9 June 2023, date of publication 14 June 2023, date of current version 18 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3286347

RESEARCH ARTICLE

Adaptive Particle Swarm Optimization With Quantum-Inspired Quantum Walks for Robust Image Security

AHMED A. ABD EL-LATIF[1,2], (Senior Member, IEEE), AND BASSEM ABD-EL-ATTY[3]

[1]EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[2]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[3]Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt

Corresponding authors: Ahmed A. Abd El-Latif (abdellatif@psu.edu.sa) and Bassem Abd-El-Atty (bassem.abdelatty@fci.luxor.edu.eg)

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

ABSTRACT In this paper, we propose a novel image cryptosystem that combines the adapted Particle Swarm Optimization (PSO) algorithm with a quantum-inspired Discrete-time Quantum Walk (DTQW). The proposed approach leverages the strengths of both PSO and DTQW, integrating them to achieve high security and efficiency in image encryption. The main contribution of this work lies in the development of this unique cryptosystem. While previous approaches have separately explored PSO or DTQW, our integration of these two techniques offers a novel and innovative approach. By employing chaotic sequences generated by a 3-D chaotic system and a controlled DTQW model, our cryptosystem demonstrates a high sensitivity to even slight changes in the original image. This sensitivity ensures that minor modifications in the plaintext lead to significant changes in the ciphertext, enhancing the system's resistance against attacks. Simulation outcomes prove that the proposed encryption mechanism has high security as well as high effectiveness.This makes it well-suited for practical implementation in a post-quantum computing era.

INDEX TERMS Image security, adaptive particle swarm optimization, chaotic maps, data security, quantum walks.

I. INTRODUCTION

Data security and privacy present a vital mission in the recent age, in which digital images are generally utilized to depict data. Digital data can be maintained by applying one of the data hiding and/or encryption approaches [1], [2], [3]. Image encryption intends to transform image data from a discernible pattern to an indiscernible style [4], [5], [6], [7].

Chaotic maps present a crucial task in developing image encryption algorithms [8], [9], [10], [11], [12]. In [8], El-Latif et al. suggested a novel S-box approach and presented its role to developing an image cryptosystem in which the offered s-box algorithm is based on a 3D chaotic system. Using a 3D bit-plane permutation, Gan et al. [9] suggested a color image encryption mechanism utilizing a 3D Chen chaotic mapping.

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

Recently, metaheuristic methods are employed extensively in various fields of our daily lives. Metaheuristic methods are categorized into nine different classes according to the reports stated in [13], [14], and [15]: social-based, chemical-based, physics-based, mathematics-based, sport-based, biology-based, swarm-based, music-based, and hybrid techniques which are mixes of those. Swarm-based methods are employed extensively in designing modern image encryption algorithms to provide high security. Based on an improved 7D hyperchaotic system, Kaur et al. [16] offered an image encryption mechanism in which an evolutionary algorithm is operated to tune the primary parameters of the hyperchaotic system. Among swarm intelligence methods are ant colony optimization, artificial bee colony, genetic algorithms, particle swarm optimization (PSO), cuckoo search algorithm, glowworm swarm optimization, etc. [17]. The PSO algorithm has many advantages, including low computational complexity, high concourse rate, and it does

not mandate an extensive number of control parameters. PSO primarily concentrates on a number of random particles and aims to frequently find the best solution. The PSO algorithm is extensively utilized to design modern image encryption algorithms to provide high security [18], [19], [20], [21]. Based on the PSO algorithm and the logistic map, Wang and Li [18] offered an image encryption mechanism in which the fitness function of operating PSO is based on information entropies and correlation coefficients to determine the final cipher image. Also, based on the PSO and the logistic map, Ahmad et al. [19] offered an image encryption mechanism in which the fitness function of operating PSO is based on the correlation coefficients to determine the final cipher image. Likewise, based on cellular automata, the PSO, and a hyperchaotic system, Zeng and Wang [20] presented an image cryptosystem in which the fitness function of operating PSO is based on the correlation coefficients to determine the final cipher image. With the efforts of designing image cryptosystems using PSO technique, the task of these optimization algorithms is to construct many cipher images for one pristine image and determine the final ciphered image based on the best values of its statistical analyses like correlation coefficients, information entropy, chi-square value, etc. Motivated by utilizing the optimization algorithms in designing cryptosystems, not optimizing the keystream by selecting good initial conditions or constructing several cipher images and selecting the final cipher image based on its performance analysis, Luo et al. [21] adapted the PSO algorithm combined with a 4D hyperchaotic system to design a novel image encryption mechanism.

However, with the fast growth of quantum computers, most of the cryptographic techniques that exist in the digital era will perhaps crack down because their structure is based on mathematical conceptions. Thus, current cryptographic techniques require quantum paradigms in their construction to resist the potential offensives from quantum machines in the immediate future.

Discrete-time quantum walk (DTQW) is assumed to be an adaptable model of quantum computation that can be adapted as a perfect key constructor because of its intrinsic non-linear chaotic dynamical properties. DTQW is like chaos, which has a high sensitivity to primary parameters and chaotic behavior, while DTQW has additional benefits like stability, nonperiodicity, and has an unlimited key space theoretically to resist various offensives [22].

Yet, efforts to realize physical quantum devices are insufficient to build large-scale quantum computers. Therefore, designing quantum algorithms is inapplicable until the availability of quantum computers. Some researchers have intended to design quantum-inspired algorithms to overcome the problem of realizing a quantum device and utilizing the power of quantum capabilities [23], [24], [25]. Regarding this dilemma, Abd-El-Atty [26] suggested a new steganographic technique for concealing medical images in public images, in which this steganographic technique is based on adapted PSO, quantum walks as a quantum-inspired model, and a 3D chaotic mapping.

In this study, we aim to use DTQW as a quantum-inspired model with chaotic maps and the adapted PSO algorithm for designing a new image cryptosystem that combines high security and efficiency with the capability to resist the potential offensives from quantum machines. The introduced cryptosystem employs a 3-D chaotic system [27] for generating three chaotic sequences ($S1$, $S2$, and $S3$) and the controlled DTQW model for generating one sequence ($S4$). The four generated sequences ($S1$, $S2$, $S3$, and $S4$) are fed into the adapted PSO algorithm, which generates two new sequences ($V1$ and $P1$), the position sequence ($P1$) being used to permute the original image and the velocity sequence ($V1$) being used in the substitution process. Simulation outcomes prove that the presented encryption mechanism has high security as well as high efficiency. To summarize the contributions of this work:

1) A novel image cryptosystem is proposed, which combines the adapted Particle Swarm Optimization (PSO) algorithm with a quantum-inspired Discrete-time Quantum Walk (DTQW). This integration leverages the strengths of both PSO and DTQW, resulting in a unique and innovative approach to image encryption.
2) The presented security approach exhibits a high sensitivity to even slight changes in the original image. By utilizing chaotic sequences generated by a 3-D chaotic system and a controlled DTQW model, the cryptosystem ensures that minor modifications in the plaintext lead to significant changes in the ciphertext. This sensitivity enhances the system's resistance against attacks, reinforcing its security.
3) The proposed cryptosystem opens the door to utilizing quantum-inspired systems with optimization mechanisms in the design of modern cryptosystems. With its high security and efficiency, as demonstrated by simulation outcomes, the cryptosystem is well-suited for practical implementation in a post-quantum computing era.

In what follows: the preliminary knowledge for a 3D chaotic mapping, DTQW model, and the adapted PSO algorithm are stated in Sec. II. The suggested image cryptosystem is given in Sec. III, while Sec. IV is devoted to the simulation outcomes. Eventually, concluding remarks are given in Sec. V.

II. PRELIMINARY KNOWLEDGE

A. 3D CHAOTIC MAPPING

Chaotic maps present an important task in developing cryptographic mechanisms because of their non-linear chaotic properties and their sensitiveness to primary key parameters. Sambas et al. [27], presented a new 3D chaotic mapping and presented its role in developing an image encryption approach. The presented chaotic system is defined as

in Eq. (1).

$$\begin{cases} x1_{t+1} = x3_t \mod 1 \\ x2_{t+1} = \left(-x3_t(ax2_t + bx2_t^2 + x1_t x3_t)\right) \mod 1 \\ x3_{t+1} = \left(x1_t^2 + x2_t^2 - |x1_t| - 1\right) \mod 1 \end{cases} \tag{1}$$

here $x1_0$, $x2_0$, and $x3_0$ are initial conditions and a, b are control parameters of the system. A detailed dynamic analysis of this system is illustrated in [27].

B. QUANTUM WALKS

Quantum walks have two classes: DTQW and continuous-time quantum walk [28]. In this research, we pay attention to DTQW, which is a perfect model of quantum walks and is suitable for designing secure cryptographic algorithms [22]. The key elements of acting DTQW on a circle are the coin particle $H_p = \cos\mu|0\rangle + \sin\mu|1\rangle$ and the walker space H_s, which both are in Hilbert space $H = H_s \otimes H_p$. In every step r of operating one-particle DTQW on a circle governed by a binary string B, the unitary transformations $\hat{T}_0$ ($\hat{T}_1$) is applied on the full quantum system $|Q\rangle$ if the value of r^{th}-bit is 0(1), respectively. If the r^{th}-step exceeds the length of B, the unitary transformation $\hat{T}_2$ is applied. $\hat{T}_0$ can be stated as given in Eq. (2) [22],

$$\hat{T}_0 = \hat{S}(\hat{I} \otimes \hat{U}_0) \tag{2}$$

where $\hat{S}$ refers the shift operator and can be represented for operating one-particle DTQW on a cycle of odd N-node as in Eq. (3).

$$\begin{aligned} \hat{S} = \sum_{i=1}^{N} & (|(i+1) \mod N, 0\rangle\langle i, 0| \\ & + |(i-1) \mod N, 0\rangle\langle i, 1|) \end{aligned} \tag{3}$$

and the operator $\hat{U}_0$ refers a 2×2 coin operator and in the public case can be expressed as in Eq. (4) [22].

$$\hat{U}_0 = \begin{pmatrix} \cos\omega_0 & \sin\omega_0 \\ \sin\omega_0 & -\cos\omega_0 \end{pmatrix} \tag{4}$$

Similar to $\hat{T}_0$, $\hat{T}_1$ and $\hat{T}_2$ can be defined using ω_1 and ω_2 where $\omega_0, \omega_1, \omega_2 \in [0, \pi/2]$. Finally, the definitive quantum state $|Q\rangle_r$ after r steps can be provided as in Eq. (5),

$$|Q\rangle_{final} = \left(\hat{T}_m\right)^r |Q\rangle_{initial} \tag{5}$$

where $m \in \{0, 1, 2\}$. The possibility of locating the walker at position i after r steps can be represented using Eq. (6).

$$P(i, r) = \left|\langle i,0| \left(\hat{T}_m\right)^r |Q\rangle_{initial}\right|^2 + \left|\langle i,1| \left(\hat{T}_m\right)^r |Q\rangle_{initial}\right|^2 \tag{6}$$

TABLE 1. Running environment description.

Item	Description
Operating system	Windows 7 64-bit
MATLAB software	R2016b
Processor	Intel® Core™ 2 CPU 3.00 GHz
RAM	4 GB

C. PARTICLE SWARM OPTIMIZATION

PSO is a hypothetical computation strategy using swarm intelligence. PSO has the optimal performance capability of social conduct; therefore, it can be employed to solve different optimization issues. PSO is commonly used in various fields such as adaptive control, machine learning, function optimization, signal processing, and neural networks due to its easy implementation, simple calculations, and optimization for problems [20], [21].

In PSO, each particle represents an individual solution. The algorithm initiates with the primary state of any particle m and utilizes two values for each particle's update: pbest (l_m) and gbest (g_m). Each particle m has main two elements: velocity (v_m) and position (p_m), which can be updated for each particle using Eq. (7) [29].

$$\begin{cases} v_{m,n}(s+1) = \beta v_{m,n}(s) + c1 \times r1_n(s)\left(l_{m,n}(s) - p_{m,n}(s)\right) \\ \qquad\qquad + c2 \times r2_n(s)\left(g_{m,n}(s) - p_{m,n}(s)\right) \\ p_{m,n}(s+1) = v_{m,n}(s+1) + p_{m,n}(s) \end{cases} \tag{7}$$

here n denotes the dimension of m, β represents the inertia coefficient, $r1$ and $r2$ are random numbers in the interval (0,1), $c1$ and $c2$ are the collective and subjective parameters.

Motivated by utilizing the PSO algorithm in designing cryptosystems, not optimizing the keystream by selecting various initial conditions or constructing several cipher images and selecting the final cipher image based on its performance analysis, we ought to adapt the PSO algorithm as presented in Eq. (8) [21].

$$\begin{cases} v_{s+1} = \beta v_s + c1 \times r1_s(l_s - p_s) + c2 \times r2_s(g_s - p_s) \\ p_{s+1} = v_{s+1} + p_s \end{cases} \tag{8}$$

where $r1$, $r2$, and l sequences are generated by iterating the 3-D chaotic mapping, while the g sequence is generated from the DTQW model.

III. PROPOSED ENCRYPTION ALGORITHM

In this part, the suggested image cryptosystem using the 3-D chaotic system, adapted PSO, and DTQW is presented. The presented cryptosystem employs the 3-D chaotic system [27] for generating three chaotic sequences ($S1$, $S2$, and $S3$) and the controlled DTQW for generating one sequence ($S4$). The generated four sequences ($S1$, $S2$, $S3$ and $S4$) are utilized as input to the PSO algorithm for constructing two new sequences ($V1$ and $P1$), in which the cycle length of the generated sequences is the size of the original

TABLE 2. Initial parameters description.

Parameter	Value	Description
$x1_0$	0.764	Initial conditions of system (1)
$x2_0$	0.549	
$x3_0$	0.276	
a	14	Control parameters of system (1)
b	3	
B	1 0 0 1 1 0 1 0 1 1 1 0 0 1 0 0 1 1 0 1 1 1 0 0 0 1 0 1 0 0 0 1 1 1 0 1 0 1 1 1 0 0 1 1 0 1 0 1 1 1 0 1 0	Controlled binary message
N	271	Number of nodes in the circle (Odd number)
r	275	Number of steps of acting DTQW
μ	0	Used to construct the coin particle
ω_0	$\pi/3$	Used to construct the unitary transformation $\hat{T}_0$
ω_1	$\pi/4$	Used to construct the unitary transformation $\hat{T}_1$
ω_2	$\pi/6$	Used to construct the unitary transformation $\hat{T}_2$
v_0	0.5	Initial velocity
p_0	1	Initial position
β	0.1	Inertia coefficient
$c1$	1	Random numbers
$c2$	1	

image. The position sequence ($P1$) is used to permutate the original image while the velocity sequence ($V1$) is used in the substitution process. For making the presented image encryption algorithm highly sensitiveness to slight changes in the pristine image, some information about the substituted image is obtained, then this information is transformed into a binary string for controlling the DTQW system and generating a new sequence ($S5$). The first three chaotic sequences ($S1$, $S2$, and $S3$) and the last sequence ($S5$) generated by DTQW are used as input for the PSO algorithm, which generates a new two sequences ($V2$ and $P2$), with the new position sequence ($P2$) used to permutate the first substituted image and the velocity sequence ($V2$) used to substitute the second permutated image to construct the final encrypted image. The outline of the presented image encryption technique is given in Fig. 1, while the detailed steps are pointed out in Algorithm 1.

IV. SIMULATION OUTCOMES

A PC with Intel® Core™ 2 CPU 3.00 GHz, RAM of 4GB, and prepared with MATLAB R2016b software is utilized to assess the presented image cryptosystem (see Table 1). The original images that were utilized to test our image cryptosystem are taken from Kodak dataset[1] and named as Macaws, Window, Chalet, and Stream each of size 768×512 (see Figure 2). The initial parameters used for acting the 3-D chaotic system (1) are set as $x1_0 = 0.764, x2_0 = 0.549, x3_0 = 0.276$, $a = 14$, and $b = 3$, while $B = [1001\ 1010\ 1110\ 0100\ 1101\ 1100\ 0101\ 0011\ 1010\ 1110\ 0110\ 1011\ 1010]$, $N = 271$, $r = 275$, $\mu = 0$, $\omega_0 = \pi/3$, $\omega_1 = \pi/4$, and $\omega_2 = \pi/6$ are devoted to operate DTQW on a circle, and the key parameters $v_0 = 0.5$, $p_0 = 1$, $\beta = 0.1$, $c1 = 1$, and $c2 = 1$ are for processing the adapted PSO algorithm (see Table 2).

[1]True Color Kodak Images, http://r0k.us/graphics/kodak/, Accessed: 10-2-2022.

A. CORRELATION ANALYSIS

To calculate the correlation coefficients for the pristine and ciphered images, we picked 10^4 pairs of neighboring pixels in each direction at random, from which the correlation coefficients can be expressed mathematically as given in Eq. (9).

$$CF = \frac{\sum_{t=1}^{M} (O_t - \bar{O})(C_t - \bar{C})}{\sqrt{\sum_{t=1}^{M} (O_t - \bar{O})^2 \sum_{t=1}^{M} (C_t - \bar{C})^2}} \tag{9}$$

here M states the whole number of selected neighboring pixel pairs, and C_t, O_t point to the adjacent pixel values. The results of correlation coefficients are declared in Table 3, in which the values for the crypto-images are very adjacent to zero. Also, Figures 3, 4, and 5 present the distribution of correlation values for each direction for the Macaws image and its corresponding encrypted version. From the results presented in Table 3 and the graphs given in Figures 3, 4, and 5, no helpful information was obtained about the original image by evaluating the correlation coefficients.

B. DIFFERENTIAL ANALYSIS

To test the sensitivity of the plain image to tiny bit modification, two tests are performed: UACI (“Unified Average Changing Intensity”) and NPCR (“Number of Pixels Change Rate”), in which they can be stated mathematically as follows.

$$\begin{aligned} NPCR &= \frac{\sum_{a;b} D(a,b)}{M} \times 100\%, \\ D(a,b) &= \begin{cases} 0 \ if \ \ Cg1(a,b) = Cg2(a,b) \\ 1 \ if \ \ Cg1(a,b) \neq Cg2(a,b) \end{cases} \end{aligned} \tag{10}$$

$$UACI = \frac{1}{M}\left(\sum_{a;b} \frac{|Cg1(a,b) - Cg2(a,b)|}{255}\right) \times 100\% \tag{11}$$

where $Cg1$, $Cg2$ are two ciphered images for one original image with tiny variations in one bit, M is the total number of pixels that exist in the image. The results of UACI and NPCR tests are stated in Table 4, which proved that any tiny variations in the original image conduct to a huge difference in the outcome ciphered image.

C. HISTOGRAM ANALYSIS

The image histogram reflects the frequency of every pixel value in the image. A well-developed image cryptosystem must safeguard the congruous distribution of dissimilar ciphered images to withstand statistical attacks. The histograms for the original and encrypted Macaws images

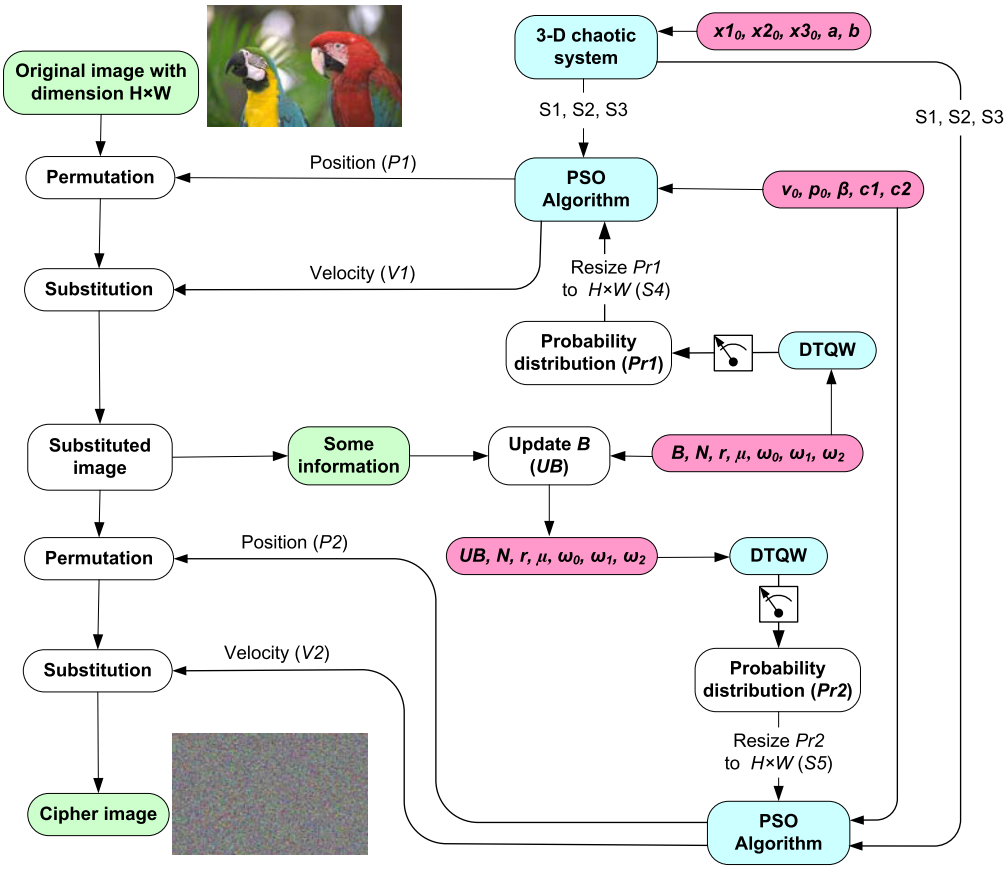

FIGURE 1. Outline of the presented image encryption procedure.

TABLE 3. Outcomes of correlation test.

Image	Dir.								
	H			V			D		
	Re.	Gr.	Bl.	Re.	Gr.	Bl.	Re.	Gr.	Bl.
Macaws	0.9869	0.9820	0.9865	0.9870	0.9863	0.9870	0.9785	0.9750	0.9794
Window	0.9555	0.9402	0.9542	0.9664	0.9623	0.9650	0.9326	0.9184	0.9284
Chalet	0.9349	0.9227	0.9201	0.9451	0.9373	0.9266	0.9123	0.8998	0.8952
Stream	0.8425	0.8495	0.8538	0.8913	0.9015	0.9054	0.8098	0.8158	0.8316
CipherMacaws	-0.0001	0.0002	0.0010	0.0004	0.0009	-0.0007	0.0009	-0.0006	-0.0004
CipherWindow	-0.0010	0.0008	-0.0007	0.0006	-0.0008	0.0003	0.0007	-0.0007	0.0004
CipherChalet	-0.0009	-0.0001	-0.0004	0.0003	0.0008	0.0003	0.0001	0.0002	0.0004
CipherStream	-0.0006	-0.0008	-0.0001	-0.0002	-0.0004	0.0002	-0.0005	-0.0009	0.0005

are displayed in Figure 6, in which the histograms of the plain images are distinguishable from each other and the histograms of their equivalent ciphered versions are like each other. Consequently, the suggested cryptosystem can withstand histogram analysis attacks.

D. INFORMATION ENTROPY ANALYSIS

Information Shannon entropy is a statistical test of the pixel value distribution per level in the image, which stated as follows:

$$E(X) = -\sum_{t=0}^{255} p(x_t) \log_2 (p(x_t)) \tag{12}$$

here $p(x_t)$ states the probability of x_t. The probable values for a greyscale image are 2^8, so the ideal value for entropy is 8-bit. Table 5 displays the outcomes of the entropy test, in which every cipher image's information entropy value is pretty near to 8 bits. Consequently, the presented cryptosystem is secure against entropy attack.

E. KEY SPACE ANALYSIS

Any well-developed cryptosystem must have a key space larger than 2^{100} to withstand brute-force raids. The presented encryption mechanism utilizes a set of key parameters ($x1_0$, $x2_0$, $x3_0$, a, b, B, N, r, μ, ω_0, ω_1, ω_2) in both the encryption and decryption algorithms, in addition to initial values of operation the adapted PSO algorithm. The key space for the bit string B seems to be infinite, but actually the key space must be finite. Assuming the computation accuracy for digital resources is 10^{-16}, then the total key space of our

Algorithm 1 Pseudocode for the Presented Image Encryption Procedure

Parameters: $x1_0, x2_0, x3_0, a, b, B, N, r, \mu, \omega_0, \omega_1, \omega_2, v_0, p_0, \beta, c1, c2$ // Here $x1_0$, $x2_0$, $x3_0$, a, and b are devoted to iterate the 3-D chaotic system (1), while B, N, r, μ, ω_0, ω_1, and ω_2 are devoted to operate the DTQW model, and the key parameters v_0, p_0, β, $c1$, and $c2$ are for processing the adapted PSO algorithm (8)

Input: Original image (Og)

Output: Cipher-image (Cg) and SP

$[H \;\; W \;\; C] \leftarrow size(Og)$// Acquire the size of the original image

$[S1 \;\; S2 \;\; S3] \leftarrow 3DChaoticSystem(x1_0, x2_0, x3_0, a, b, H \times W \times C)$// Act the chaotic map (1) for $H \times W \times C$ times

$Pr1 \leftarrow DTQW(B, N, r, \mu, \omega_0, \omega_1, \omega_2)$ // Act DTQW on a circle of N-node for r steps and governed by the binary message B, where the primary particle is $H_p = \cos\ \mu|0\rangle + \sin\ \mu|1\rangle$, ω_0, ω_1, and ω_2 are utilized to construct $\hat{T}_0$, $\hat{T}_1$, and $\hat{T}_2$, respectively

$S4 \leftarrow Resize(Pr1, [1 \;\; H \times W \times C])$ // transform the probability distribution vector $Pr1$ of length N to a vector of length $H \times W \times C$

// Process the adapted PSO algorithm (8)

for $t \leftarrow 1$ *to* $H \times W \times C$ **do**

  $v1_{t+1} \leftarrow \beta \times v1_t + c1 \times S1_t(S3_t - p1_t) + c2 \times S2_t(S4_t - p1_t)$;

  $p1_{t+1} \leftarrow v1_{t+1} + p1_t$;

$Ps \leftarrow sort(P1)$// Order the components of $P1$ in ascending arrangement

$PVec1 \leftarrow index(P1 \;\; in \;\; Ps)$// Get the index for each component of $P1$ in Ps

$OgVec \leftarrow reshape(Og, 1, H \times W \times C)$ // transform the original image to a vector

for $t \leftarrow 1$ *to* $H \times W \times C$ **do**

  $PgVec1(t) \leftarrow OgVec(PVec1(t))$ // permutation process

$Key1 \leftarrow floor(V1 \times 10^{14}) \mod 256$// Transform $V1$ sequence into integers

$SgVec \leftarrow PgVec1 \oplus Key1$// substitution process

$SP \leftarrow \sum_{t \leftarrow 1}^{H \times W \times C} SgVec(t)$// Obtain some information about $SgVec$ image

$UB \leftarrow [B \;\; de2bi(SP)]$// Append the binary string resulting from $de2bi(SP)$ at the end of B

$Pr2 \leftarrow DTQW(UB, N, r, \mu, \omega_0, \omega_1, \omega_2)$;

$S5 \leftarrow Resize(Pr2, [1 \;\; H \times W \times C])$;

for $t \leftarrow 1$ *to* $H \times W \times C$ **do**

  $v2_{t+1} \leftarrow \beta \times v2_t + c1 \times S1_t(S3_t - p2_t) + c2 \times S2_t(S5_t - p2_t)$;

  $p2_{t+1} \leftarrow v2_{t+1} + p2_t$;

$Ps \leftarrow sort(P2)$;

$PVec2 \leftarrow index(P2 \;\; in \;\; Ps)$;

for $t \leftarrow 1$ *to* $H \times W \times C$ **do**

  $PgVec2(t) \leftarrow SgVec(PVec2(t))$;

$Key2 \leftarrow floor(V2 \times 10^{14}) \mod 256$;

$CgVec \leftarrow PgVec2 \oplus Key2$;

$Cg \leftarrow reshape(CgVec, H, W, C)$// Final cipher image

TABLE 4. Outcomes of UACI and NPCR testes.

Image	UACI	NPCR
Macaws	33.49142%	99.61539%
Window	33.46430%	99.61480%
Chalet	33.49918%	99.61649%
Stream	33.48178%	99.61039%

encryption mechanism is 10^{192}, which is acceptable for any cryptosystem.

TABLE 5. Outcomes of entropy test.

Image	Original	Cipher
Macaws	7.601941	7.999837
Window	7.309858	7.999839
Chalet	7.136653	7.999865
Stream	7.560696	7.999851

F. KEY SENSITIVITY ANALYSIS

Key sensitivity test is a crucial measure to prove the security of any cryptographic application. To checking the

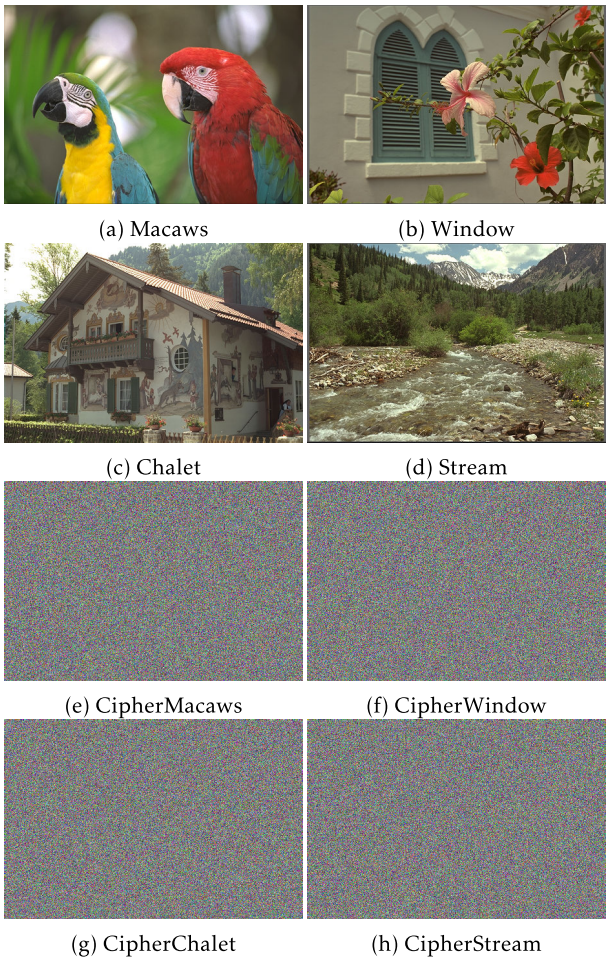

FIGURE 2. Original images and their corresponding cipher ones.

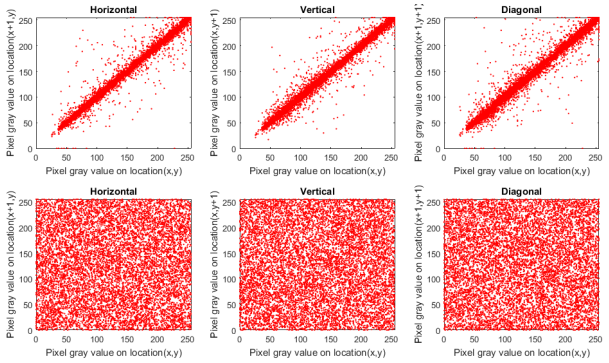

FIGURE 3. Distribution of correlation values per direction for the red component of the Macaws image, in which the diagrams in the first row are for the original image and the plots in the other row are for the corresponding cipher image.

sensitivity of the secret keys to the decrypt effects, the CipherMacaws image is decrypted numerous times with slight modifications in the actual secret keys, as shown in Figure 7. According to the results shown in Figure 7, the offered image encryption mechanism has a high sensitivity for the secret key parameters.

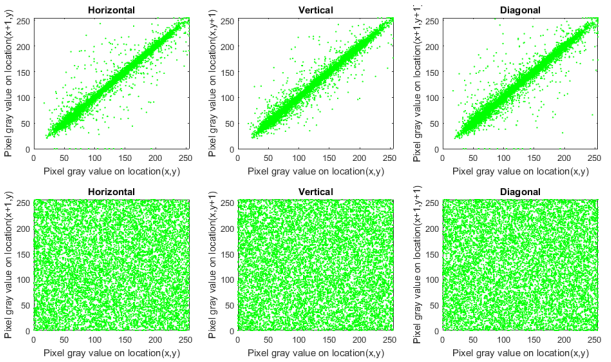

FIGURE 4. Distribution of correlation values per direction for the green component of the Macaws image, in which the diagrams in the first row are for the original image and the plots in the other row are for the corresponding cipher image.

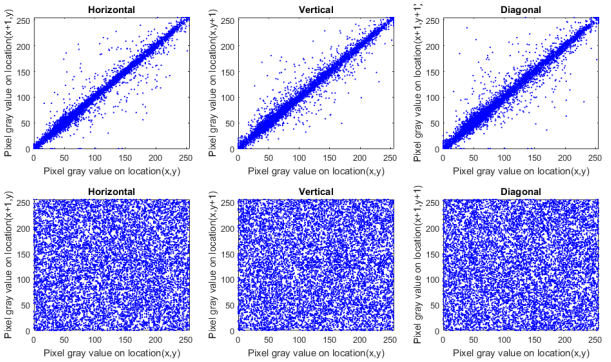

FIGURE 5. Distribution of correlation values per direction for the blue component of the Macaws image, in which the diagrams in the first row are for the original image and the plots in the other row are for the corresponding cipher image.

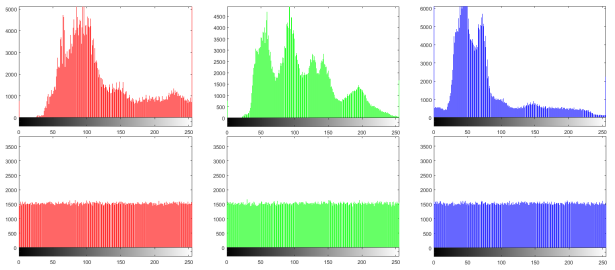

FIGURE 6. Histograms of Macaws image, in which the top row indicates the image before encryption and the other row represents the image after encryption.

G. COMPLEXITY ANALYSIS

The performance of the presented mechanism is evaluated from two viewpoints: time complexity and space complexity. The space complexity of a cryptosystem is the amount of memory required to encrypt an image of dimensional $h \times w$ using that cryptosystem. The suggested cryptosystem consists of two sequential rounds, and each round consists of a key generation phase, permutation phase, and substitution phase. At first, the 3-D chaotic system is iterated hw times, then DTQW acts on a circle of N-node, which requires $\mathcal{O}(N^2)$ of computational complexity. After that, the adapted PSO system is iterated hw times. Therefore, the total space complexity of the key generation phase is

(a) The actual key
(b) The actual key except $x1_0 = 0.7640000000000001$
(c) The actual key except $a = 14.000000000000001$
(d) The actual key except $N = 273$
(e) The actual key except $r = 274$
(f) The actual key except $v_0 = 2$
(g) The actual key except removing the first bit of B
(h) The actual key except removing the last bit of B
(i) The actual key except first bit of B from 1 to 0

FIGURE 7. Decrypted image Macaws several times with tiny changes in the actual secret keys.

$\mathcal{O}(\max(N^2, hw))$. The permutation phase is based on arranging the elements of sequence $P1$ and obtaining the index of each component, which requires $\mathcal{O}(hw \log hw)$ computational complexity, while the substitution phase consists of the bit-XOR process. Finally, the total space complexity of the suggested encryption mechanism is $\mathcal{O}(\max(hw \log hw, N^2))$.

To evaluate the suggested mechanism from the time complexity perspective, Table 6 states the time taken to encrypt gray-scale images of various dimensions compared to other related mechanisms as reported in [8], [9], [21], [30], [31], and [32]. From the stated data in Table 6 and the stated space complexity, we can deduce that our encryption mechanism can be utilized in real-time applications.

TABLE 6. Encryption time (in seconds).

Mechanism	Image dimension		
	256×256	512×512	1024×1024
Proposed	0.0951	0.4417	1.9329
[8]	0.2981	1.3049	0.5270
[30]	0.2224	0.9731	3.9177
[31]	0.6347	2.4913	9.9185
[32]	0.1272	0.5156	2.1321
[9]	5.3500	-	-
[21]	0.0913	0.4219	1.8134

TABLE 7. Statistical analyses of Encrypted AllWhite and Encrypted AllBlack images.

Image	Entropy	Correlation		
		H	V	D
Encrypted AllWhite	7.999392	0.0003	-0.0002	-0.0001
Encrypted AllBlack	7.999293	0.0008	-0.0004	-0.0004

H. TYPICAL ATTACKS ANALYSIS

According to Kerckhoff's principle, the cryptanalyst knows everything about the cryptosystem under study except the secret keys. A well-developed cryptosystem must withstand typical attacks, including known-plaintext, ciphertext-only, chosen-ciphertext, and chosen-plaintext attacks [24]. In these attacks, the cryptanalyst can select a chosen pristine image by performing the chosen-ciphertext attack, and the encrypted image can be obtained based on the encryption algorithm in an attempt to extract some information about the secret keys or to develop a technique to decrypt the cipher images without requiring secret keys. Accordingly, the most powerful attack is the chosen-plaintext attack, hence, if a cryptosystem can

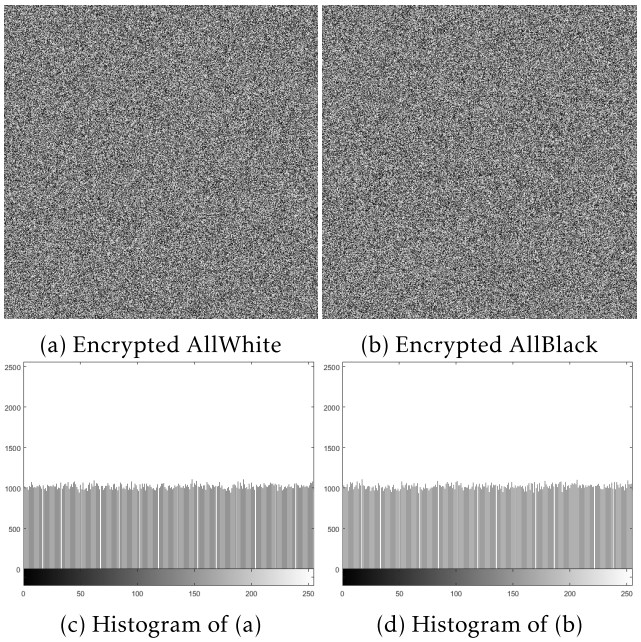

FIGURE 8. Corresponding ciphered images for allWhite and allBlack images and their histograms.

withstand this attack, it also has the ability to withstand the other three attacks. The suggested cryptosystem consists of two sequential rounds, and each round consists of a key generation phase, a permutation phase, and a substitution phase. The key generation phase in the first round of the suggested cryptosystem is based only on the secret key, while in the second round its construction is based on the substituted image from the first round plus the initial secret key, in which any tiny changes in the original image lead to a gigantic difference in the outcome ciphered image. Some cryptoanalysts commonly utilize special images, such as allWhite or allBlack images, to violate the cryptosystem. The corresponding cipher images for allWhite and allBlack images of dimension 512×512 and their histograms are provided in Fig. 8, which are both noise-like. Moreover, some statistical test results are stated in Table 7. From the stated results in Fig. 8 and Table 7, no useful information can be obtained by performing the chosen-ciphertext attack.

I. DATA LOSS ANALYSIS

The transmitted data might miss some of its parts when it transfers over a communication channel. Accordingly, a good-designed encryption algorithm ought to have the fitness to withstand data loss attacks. To appraise the offered cryptosystem against data loss attacks, some slices of the ciphered image were cut out and tried to recover the original image from the deficient encrypted image through the deciphring process. Figure 9 provides the results of data loss offensives, in which the secret image is efficiently gained without renouncing information in the cut part.

J. DISCUSSIONS

The presented mechanism was analyzed from two perspectives: performance and robustness to withstand different attacks, including differential, statistical, brute force, and occlusion attacks. From the viewpoint of performance, the presented mechanism is evaluated from two perspectives of complexity: space complexity and time complexity. The total space complexity of the suggested encryption mechanism is $\mathcal{O}(\max(N^2, hw \log hw))$, while Table 6 stated the time taken to encrypt gray-scale images of various dimensions compared to other related mechanisms. From the stated outcomes, we can conclude that our encryption mechanism can be utilized in real-time applications.

From the viewpoint of withstanding different attacks, Table 3 stated the outcomes of correlation coefficients, in which the values for the crypto-images are very adjacent to zero. Also, Figures 3, 4, and 5 present the distribution of correlation values per direction for the Macaws image and its corresponding ciphered version. From the outputs presented in Table 3 and the plots given in Figs. 3, 4, and 5, no helpful information was obtained about the original image via evaluating the correlation coefficients. To esteem the sensitivity of the original image to tiny bit modification, UACI and NPCR tests were performed. The outcomes of those tests are recorded in Table 4, in which ascertained that any tiny variations in the plain image led to a giant difference in the outcome ciphered image. Figure 6 displayed the histograms for the original and encrypted Macaws images, in which the histograms of the original image are dissimilar from each other and the histograms of their equivalent encrypted versions are like each other. Regarding entropy attacks, Table 5 displays the outcomes of the entropy test, in which every cipher image's information entropy value is pretty near to 8 bits. Regarding brute force attacks, the whole key space of the suggested cryptosystem is 10^{192}, which is acceptable for any cryptosystem. To test the sensitivity of the secret key to the decrypt effects, the CipherMacaws image is decrypted numerous times with tiny modifications in the actual secret keys, as shown in Figure 7, in which the offered cryptosystem has a high sensitivity for the initial parameters. The suggested cryptosystem consists of two sequential rounds, and each round consists of a key generation phase, a permutation phase, and a substitution phase. The key generation phase in the first round of the suggested cryptosystem is based only on the secret key, while in the second round its construction is based on the substituted image from the first round plus the initial secret key, in which any tiny variations in the pristine image causing to a gigantic difference in the outcome ciphered image. Hence, the suggested cryptosystem has the capability to withstand the typical attacks. To appraise the suggested cryptosystem against data loss offensives, some slices of the ciphered image were cut out and tried to recover the original image from the deficient encrypted image through the deciphring process. Figure 9 provided the effects of data loss offensives, in which the secret image is efficiently gained without

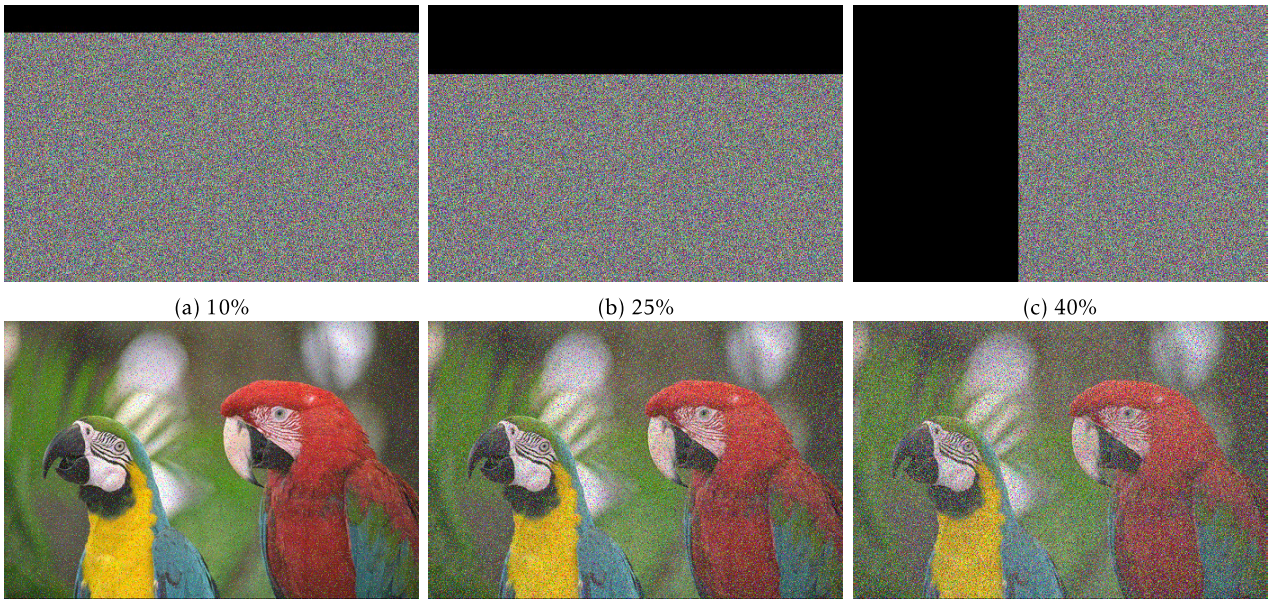

FIGURE 9. Results of data loss offensives, in which the first tuple presents the deficient ciphered images by removing out some of its slices and the second tuple presents the analogous decrypted images.

TABLE 8. Average values of correlation, NPCR, UACI, information entropy of the suggested cryptosystem with their corresponding values declared in [9], [10], [11], [12], [20], [33], and [34].

Algorithm	Correlation			NPCR	UACI	Information entropy
	H	V	D			
Proposed	-0.00022	0.00014	0.00001	99.6143%	33.4842%	7.99985
[33]	0.00219	0.00169	0.00186	99.6110%	33.4757%	7.99929
[34]	-0.00420	-0.00490	-0.00450	99.6101%	33.5252%	7.99950
[20]	0.00530	-0.00890	0.01260	99.6352%	33.5614%	7.99870
[9]	-0.00970	-0.00870	0.00650	99.6000%	33.4400%	7.99700
[10]	0.00052	0.00033	0.00087	99.6096%	33.4596%	7.99930
[11]	0.00050	0.00170	-0.00250	99.6067%	33.4267%	7.99866
[12]	0.00180	-0.00161	0.00463	99.6225%	33.5950%	7.99301

losing information in the cutting part. Finally, to guarantee the efficacy of the offered encryption mechanism alongside other corresponding cryptosystems, Table 8 presents the correlation, NPCR, UACI, and global entropy average values of the suggested cryptosystem with their corresponding values declared in [9], [10], [11], [12], [20], [33], and [34]. From the values given in Tables 6 and 8, we can infer the efficacy of the offered cryptosystem compared to the corresponding mechanisms.

V. CONCLUSION AND FUTURE RESEARCH

This paper has successfully achieved its primary objective of exploring the integration of quantum paradigms and optimization algorithms to develop modern cryptosystems that offer high security and efficiency. Through the introduction of a novel image encryption approach that combines chaotic maps, the Particle Swarm Optimization (PSO) algorithm, and the Discrete-time Quantum Walk (DTQW), this paper presents a robust cryptographic mechanism capable of withstanding both quantum machines and digital attacks. The simulation results validate the effectiveness and high security of the proposed encryption approach, thereby affirming its suitability for real-time applications. However, it is important to acknowledge that the scope of this paper is limited to securing image data types, and its applicability to other data types such as videos, text, etc., remains unexplored. Future research endeavors will focus on leveraging soft computing architectures and quantum-inspired quantum walks to design novel video encryption approaches specifically tailored for Internet of Things (IoT) applications. These advancements aim to provide enhanced security measures capable of withstanding potential offensives from both quantum and digital machines.

REFERENCES

[1] S. Yi, Y. Zhou, and Z. Hua, "Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion," *Signal Process., Image Commun.*, vol. 64, pp. 78–88, May 2018.
[2] B. Carpentieri, A. Castiglione, A. D. Santis, F. Palmieri, and R. Pizzolante, "One-pass lossless data hiding and compression of remote sensing data," *Future Gener. Comput. Syst.*, vol. 90, pp. 222–239, Jan. 2019.
[3] C.-H. Yang, C.-Y. Weng, and J.-Y. Chen, "High-fidelity reversible data hiding in encrypted image based on difference-preserving encryption," *Soft Comput.*, vol. 26, no. 4, pp. 1–16, 2022.
[4] Y. Y. Ghadi, S. A. Alsuhibany, J. Ahmad, H. Kumar, W. Boulila, M. Alsaedi, K. Khan, and S. A. Bhatti, "Multi-chaos-based lightweight image encryption-compression for secure occupancy monitoring," *J. Healthcare Eng.*, vol. 2022, pp. 1–14, Nov. 2022.
[5] F. Ahmed, M. U. Rehman, J. Ahmad, M. S. Khan, W. Boulila, G. Srivastava, J. C.-W. Lin, and W. J. Buchanan, "A DNA based colour image encryption scheme using a convolutional autoencoder," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 19, no. 3s, pp. 1–21, Oct. 2023.

[6] A. Ullah, A. A. Shah, J. S. Khan, M. Sajjad, W. Boulila, A. Akgul, J. Masood, F. A. Ghaleb, S. A. Shah, and J. Ahmad, "An efficient lightweight image encryption scheme using multichaos," *Secur. Commun. Netw.*, vol. 2022, pp. 1–16, Oct. 2022.
[7] F. Masood, J. Masood, L. Zhang, S. S. Jamal, W. Boulila, S. U. Rehman, F. A. Khan, and J. Ahmad, "A new color image encryption technique using dna computing and chaos-based substitution box," *Soft Comput.*, vol. 26, n0. 16, pp. 1–17, 2021.
[8] A. A. A. El-Latif, B. Abd-El-Atty, A. Belazi, and A. M. Iliyasu, "Efficient chaos-based substitution-box and its application to image encryption," *Electronics*, vol. 10, no. 12, p. 1392, Jun. 2021.
[9] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111–7130, May 2018.
[10] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.
[11] S. Askar, A. Karawia, A. Al-Khedhairi, and F. Al-Ammar, "An algorithm of image encryption using logistic and two-dimensional chaotic economic maps," *Entropy*, vol. 21, no. 1, p. 44, Jan. 2019.
[12] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, Oct. 2015.
[13] S. Akyol and B. Alatas, "Plant intelligence based metaheuristic optimization algorithms," *Artif. Intell. Rev.*, vol. 47, no. 4, pp. 417–462, May 2016.
[14] B. Alatas and H. Bingol, "Comparative assessment of light-based intelligent search and optimization algorithms," *Light Eng.*, vol. 28, no. 6, Dec. 2020.
[15] H. Bingol and B. Alatas, "Chaos based optics inspired optimization algorithms as global solution search approach," *Chaos, Solitons Fractals*, vol. 141, Dec. 2020, Art. no. 110434.
[16] M. Kaur, D. Singh, and V. Kumar, "Improved seven-dimensional (i7D) hyperchaotic map-based image encryption technique," *Soft Comput.*, vol. 26, pp. 1–10, Jan. 2022.
[17] S. Dhawan, R. Gupta, A. Rana, and S. Sharma, "Various swarm optimization algorithms: Review, challenges, and opportunities," in *Soft Computing for Intelligent Systems*. Singapore: Springer, 2021, pp. 291–301.
[18] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Opt. Lasers Eng.*, vol. 137, Feb. 2021, Art. no. 106393.
[19] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, "An image encryption approach using particle swarm optimization and chaotic map," *Int. J. Inf. Technol.*, vol. 10, no. 3, pp. 247–255, Jan. 2018.
[20] J. Zeng and C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Secur. Commun. Netw.*, vol. 2021, pp. 1–15, Feb. 2021.
[21] Y. Luo, X. Ouyang, J. Liu, L. Cao, and Y. Zou, "An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system," *Soft Comput.*, vol. 26, no. 11, pp. 5409–5435, Jan. 2022.
[22] B. Abd-El-Atty, A. A. A. El-Latif, and S. E. Venegas-Andraca, "An encryption protocol for NEQR images based on one-particle quantum walks on a circle," *Quantum Inf. Process.*, vol. 18, no. 9, p. 272, Jul. 2019.
[23] B. Abd-El-Atty, M. ElAffendi, and A. A. A. El-Latif, "A novel image cryptosystem using Gray code, quantum walks, and Henon map for cloud applications," *Complex Intell. Syst.*, vol. 9, no. 11, pp. 609–624, Jul. 2022.
[24] B. Abd-El-Atty, "Quaternion with quantum walks for designing a novel color image cryptosystem," *J. Inf. Secur. Appl.*, vol. 71, Dec. 2022, Art. no. 103367.
[25] B. Abd-El-Atty, "Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem," *Complex Intell. Syst.*, vol. 2023, pp. 1–9, Feb. 2023.
[26] B. Abd-El-Atty, "A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks," *Neural Comput. Appl.*, vol. 35, pp. 773–785, Sep. 2022.
[27] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, B. Abd-El-Atty, A. A. A. El-Latif, O. Guillén-Fernández, Sukono, Y. Hidayat, and G. Gundara, "A 3-D multi-stable system with a peanut-shaped equilibrium curve: Circuit design, FPGA realization, and an application to image encryption," *IEEE Access*, vol. 8, pp. 137116–137132, 2020.
[28] S. E. Venegas-Andraca, "Quantum walks: A comprehensive review," *Quantum Inf. Process.*, vol. 11, no. 5, pp. 1015–1106, Jul. 2012.
[29] A. Adeli and A. Broumandnia, "Image steganalysis using improved particle swarm optimization based feature selection," *Appl. Intell.*, vol. 48, no. 4, pp. 1609–1622, Aug. 2017.
[30] A.-V. Diaconu, "Circular inter-intra pixels bit-level permutation and chaos-based image encryption," *Inf. Sci.*, vols. 355–356, pp. 314–327, Aug. 2016.
[31] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.
[32] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov. 2019.
[33] X. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.
[34] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology (HIT), Harbin, China, in 2013. He is currently an Associate Professor in computer science with Menoufia University and the EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia. He is the author or coauthor of more than 240 papers, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He involved in government and international funded research and development projects related to the widespread use of artificial intelligence for 5G/6G networks. His research interests include multimedia content encryption, 5G/6G wireless communications, the IoT, cryptography, information hiding, biometrics, image processing, and quantum information processing. He is a member of ACM. He is a fellow of the Academy of Scientific Research and Technology, Egypt. He received many awards, State Encouragement Award in Engineering Sciences, in 2016, Arab Republic of Egypt; the Best Ph.D. Student Award from HIT, in 2013; and Young Scientific Award, Menoufia University, in 2014. He is the chair/co-chair/program chair of some Scopus/EI conferences. He is also the Editor-in-Chief of *International Journal of Information Security and Privacy* and a Series Editor of *Advances in Cybersecurity Management* (https://www.routledge.com). Also, he is an academic editor/associate editor for set of indexed journals (Scopus journals' quartile ranking). Currently, he had many books, more than ten books, in several publishers in Springer, IET, CRC Press, IGI-Global, Wiley, and IEEE.

BASSEM ABD-EL-ATTY received the B.S. degree in physics and computer science and the M.Sc. and Ph.D. degrees in computer science from Menoufia University, Egypt, in 2010, 2017, and 2020, respectively. He is currently an Assistant Professor with the Faculty of Computers and Information, Luxor University, Egypt. He is the author or coauthor of more than 40 papers, including refereed IEEE/Springer/Elsevier journals, conference papers, and book chapters. He is a reviewer in a set of reputable journals in Elsevier and Springer. His research interests include quantum information processing and image processing.