Hindawi
Complexity
Volume 2021, Article ID 9424469, 16 pages
https://doi.org/10.1155/2021/9424469

Research Article

A Multi-Image Cryptosystem Using Quantum Walks and Chebyshev Map

Bassem Abd-El-Atty,[1] **Abdullah M. Iliyasu**,[2,3,4] **and Ahmed A. Abd El-Latif**[5]

[1] *Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt*
[2] *Electrical Engineering Department, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia*
[3] *School of Computing, Tokyo Institute of Technology, Yokohama 226-8502, Japan*
[4] *School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China*
[5] *Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shibin Al Kawm 32511, Egypt*

Correspondence should be addressed to Abdullah M. Iliyasu; amiliyasuz@gmail.com and Ahmed A. Abd El-Latif; a.rahiem@gmail.com

Received 29 April 2021; Accepted 7 October 2021; Published 18 October 2021

Academic Editor: Leo Y. Zhang

The ubiquity of image and video applications in our daily lives makes data security and privacy prominent concerns for everyone. Among others, various image cryptosystems are relied upon to provide the necessary safeguards. With the inevitable realisation of quantum computing hardware, however, the anticipated quantum supremacy entails effortless violation of the integrity of even the best cryptosystems. Quantum walks (QWs) utilise the potent properties of quantum mechanics to provide randomness via stochastic transitions between states. Our study exploits these properties of QWs to design a multi-image cryptosystem. Furthermore, we infuse the symmetricity and orthogonality of Chebyshev maps into the QWs to realise a powerful cryptosystem that guarantees data integrity, authentication, and anonymity of the resulting images. These properties are validated via extensive simulation-based experiments that produce average values of NPCR as 99.606%, UACI as 33.45%, global entropy as 7.9998, and chi-square test as 238.14. Therefore, the proposed cryptosystem provides ordnance to protect images from illicit tampering during the era.

1. Introduction

Today, data security and privacy are integral to our daily lives where more than 300 million images are unloaded on the internet daily [1]. Mylio, software company, estimates that 9.3 trillion images will be stored online by 2022 [2]. Considering the varying levels of confidentiality and precious memories in these images, their security and privacy is a major concern to many of us.

Presently, various technologies and cryptographic mechanisms are employed to encrypt, watermark, and secure these images including the use of steganographic data hiding schemes. While data encryption pervades access to unauthorised users by making such images unintelligible, chaotic systems exhibit sensitive dependence on original conditions, which implies that, for any small alteration, the dynamics of the system persistently magnifies the original conditions. This according to [3] implies that “two trajectories with initial conditions that are arbitrarily close will diverge at an exponential rate.” There are many single-image cryptosystems that have been proposed, including those based on colour codes [4], dynamic filtering [5], imitating jigsaw method [6], bit-level permutation [7], DNA sequence operation [8], and particle swarm optimization [9], besides chaos-based image cryptosystems.

Meanwhile, there are two major classifications of chaotic maps: one- and multi-dimensional chaotic systems. One-dimensional (1D) chaotic maps offer low computational complexity, simple architecture, and structure as well as accelerated processing [10]. Despite the enumerated properties, 1D chaotic systems are exposed to attacks due to their small key space and the chaotic discontinuous ranges of their primary values [11].

Due to the developments in communication networks and prevalence of bulk data processing, multiple-image cryptosystems potentially have important roles in data security and privacy in the emerging era of big data whereas single-image cryptosystems can be utilised to protect multiple images in a per process approach, but these processes pile up to reduce the effectiveness of encryption scheme [12]. To enhance this, various scholars have invested in utilising multi-image cryptosystems to protect multiple images. In doing so, the highlighted properties of chaotic systems are exploited to design multiple-image encryption schemes with many seemingly tamper-proof cryptosystems realised [13–19]. For example, in [13], Shao et al. presented a new multiple-image encryption mechanism using logistic map and quaternion gyrator transform, while in [14], Zarebnia et al. suggested a multi-image encryption approach using chaotic maps and cyclic shift operation. Furthermore, in [15], Li et al. proposed a multi-image encryption approach in wavelet transformation domain based on a chaotic map. Similarly, in [18], Zhang and Wang presented a multi-image encryption mechanism using piecewise linear chaotic map and mixed image elements. While the highlighted schemes offer platforms to secure the images, our push towards the triple-S (speed, security, and size) limits of today's technologies compels the need for more advanced computing infrastructure.

Quantum computers offer the promise of information processing beyond the capabilities of even the best of today's supercomputers. The inevitable realisation of such hardware portends huge implications for available cryptosystems, making them vulnerable to many types of violations [20, 21]. Consequently, it is important to consider integrating this apparent "quantumness" into existing schemes to safeguard the confidentiality and integrity of images.

Quantum walks (QWs), which are quantum computing equivalents of the classical (i.e., nonquantum, or digital) random walks, provide high sensitivity to initial parameters and astounding nonperiodicity [22]. Furthermore, they exhibit significant stability and theoretically infinite key space allowance. These properties arise through reversible unitary evolution, nonrandom, quantum superposition of states, and collapse of the wave function due to state measurements [22]. The use of quantum walks in building efficient cryptosystems has been explored in many studies [20, 21, 23–25]. Moreover, QWs have been used to construct exponential speed up algorithms, quantum simulations, universal quantum gates, etc. [22].

For example, in [23], Vlachou et al. proposed a public cryptographic system that utilises QW to generate a public key, which is similar to its use by Yang et al. to propose an image encryption approach based on QW in [25]. In their contribution [20], Abd-El-Atty et al. considered an optical image encryption based on QW. Specifically, they used the alternate QW in a dual encryption strategy that, first, uses double random phase encoding that is executed using permutation followed by substitution, and second, generation of random masks.

Similarly, in [8], Yan and Li utilised the controlled alternate QWs and DNA sequence operations for colour image encryption. They used controlled alternate QWs to generate pseudorandom number generator and two rounds of DNA operation rules to encrypt plaintext images. Furthermore, in [26], Shi et al. proposed a quantum blind signature approach with cluster states using a QW-based cryptosystem. They claim that in the initial signing and verification phases, a message encrypted using QW is sent to the receiver, who requests a blind signature. Subsequently, in the verification phase, the authenticity and integrity of the transmitted message is verified. Finally, in [27], Abd El-Latif et al. considered the use of cascaded QWs with induced chaotic dynamics for cryptographic purposes. Their scheme utilised QWs to construct substitution boxes and provide the necessary chaos inducement and random number generation; the properties they claimed were combined in their reported cryptosystem. Furthermore, the schemes in [20, 27] report high encryption speeds relative to those in competing studies.

Notwithstanding the performances of the highlighted schemes, a common problem with the use of chaotic systems in the reported schemes is the low stability due to periodicity of the chaotic mapping. Meanwhile, Chebyshev polynomials satisfy the two important properties of semigroup membership and chaos. For this, our proposed cryptosystem infuses the symmetric and correlational properties of Chebyshev maps [28] to permutate the composite image. Additionally, as a prelude to realising the cipher composite image, Chebyshev mapping is used to substitute the composite image. To further elucidate, the key contributions of this study include the following:

(1) Integrating quantum walks with existing chaotic systems to design a multiple-image cryptosystem for safeguarding the confidentiality and integrity of images

(2) Using QW to substitute the composite image and update encryption key parameters

The performance of our systems is validated via extensive simulation-based experiments to establish its effectiveness and reliability in cryptographic applications involving multiple images.

The remainder of the paper is organised as follows: background on both quantum walks, and Chebyshev maps are briefly highlighted in Section 2. Intrigues regarding the use of QWs and Chebyshev mapping to design our proposed cryptosystem are presented in Section 3, while evaluation of the performance of the proposed system is reported and discussed in Section 4. Section 5 concludes this study.

2. Preliminary Background on Quantum Walks and Chebyshev Map

This section presents brief overview of the main building blocks of our proposed cryptosystem (i.e., quantum walks and Chebyshev map).

2.1. Quantum Walks. Exploiting the essential properties of quantum mechanics, notably superposition, unitarity of state evolution, and wave function collapse [29], quantum walks were proposed as equivalents of the classical random walks.

There are two core elements of QWs: coin particle $H_c = \cos\mu|0\rangle + \sin\mu|1\rangle$ and walker space H_p, both of which exist in a Hilbert space $H = H_p \otimes H_c$ [22]. To transform the full quantum state, the evolution operator $\widehat{U}$, defined in the following equation, is applied on the full quantum state:

$$\widehat{U} = \widehat{S}(\widehat{I} \otimes \widehat{C}), \tag{1}$$

where $\widehat{S}$ implies the shift operator and it is depending on the coin system of the walker. Further, the shift operators $\widehat{S}$ of one-walker QW on a cycle of V nodes can be expressed as

$$\widehat{S} = |(x-1)\mathrm{mod}V, 1\rangle\langle x, 1| + |(x+1)\mathrm{mod}V, 0\rangle\langle x, 0|. \tag{2}$$

Additionally, a 2×2 coin operator, $\widehat{C}$, can be expressed as

$$\widehat{C} = \begin{pmatrix} \cos\omega & \sin\omega \\ \sin\omega & -\cos\omega \end{pmatrix}. \tag{3}$$

Hence, the final state $|\psi\rangle_t$ after t steps can be stated as follows:

$$|\psi\rangle_t = (\widehat{U})^t |\psi\rangle_0, \tag{4}$$

where $|\psi\rangle_0$ indicates the primary state of the quantum system. Consequently, the probability of locating the particle at location x after t steps can be computed by making use of

$$P(x,t) = \left|\langle x,0|(\widehat{U})^t|\psi\rangle_0\right|^2 + \left|\langle x,1|(\widehat{U})^t|\psi\rangle_0\right|^2. \tag{5}$$

2.2. Chebyshev Map. Chebyshev polynomials are two sequences of polynomials built on the sine and cosine functions, notated as $T_n(x)$ and $U_n(x)$. These polynomials exhibit two important properties of semigroup and chaos. Of particular interest are mappings of Chebyshev polynomials for $a \longrightarrow T_n(a)$ since any pair of such mappings commute and $T_n \Diamond T_m = T_{nm}$.

The structure of the described collection of mappings, known as Chebyshev map [28, 30], is among the widely used one-dimensional chaos systems, which is expressed as

$$x_{i+1} = \cos(B \times \arccos(x_i)), \tag{6}$$

where $x_i \in [-1, 1]$ is the original value of the chaotic map and $B \in N$ is the control parameter and $B \geq 2$.

3. Proposed Cryptosystem

This section outlines the use of the quantum walks and Chebyshev map highlighted in the previous section to design our proposed multiple-image cryptosystem. In summary, the proposed scheme involves the use of QW to substitute the plain composite image and the use of the substituted composite image to update key parameters of the Chebyshev map and subsequent permutation of the substituted composite image using QW and Chebyshev map. Finally, this permutated image is substituted using the Chebyshev map to realise the cipher composite image.

3.1. Encryption Algorithm. Figure 1 presents a graphical outline of the proposed encryption approach which is executed in the steps enumerated as follows:

(1) Merge all plain images (*Ig*01, *Ig*02, . . ., *Ig*0*N*) into one composite image (Pim), and then convert Pim into a vector ImVec.

$$\mathrm{ImVec} = \mathrm{reshape}\,(Pim, m \times n \times c, 1), \tag{7}$$

where m, n, and c are the dimension of the composite image.

(2) Select the primary key parameters (V, t, μ, and ω) for operating QWs t times on a cycle of odd V nodes to produce a probability distribution P of size V. Here, the primary state of the coin walker is $H_c = \cos\mu|0\rangle + \sin\mu|1\rangle$, and ω is used to construct the coin operator $\widehat{C}$ (equation (3)), where $\mu, \omega \in [0, (\pi/2)]$.

(3) Resize P to the dimension of the composite image ImVec ($m \times n \times c$). This action accommodates composite images of different dimensions. In this study, the bicubic interpolation method [31] is used for the resizing process.

$$\mathrm{Re}\,P = \mathrm{resize}\,(P, [\,m \times n \times c \quad 1\,]). \tag{8}$$

(4) Obtain the key sequence (Key1) via conversion of ReP into integer values.

$$\mathrm{Key1} = \mathrm{floor}\left(\mathrm{Re}\,P \times 10^{12}\right)\mathrm{mod}256, \tag{9}$$

where floor is the floor operation that rounds each value of $\mathrm{Re}\,P \times 10^{12}$ towards zero (e.g., floor $(4.736) = 4$).

(5) Execute the Bitwise XOR operation process on the composite image ImVec and key1 to obtain the substituted composite image SimVec as

$$\mathrm{SimVec} = \mathrm{ImVec} \oplus \mathrm{Key1}. \tag{10}$$

(6) Select the primary key parameters (x_0, B) for the Chebyshev map, and then update the initial key parameter x_0 as specified in the following equations:

$$\delta = \frac{\sum_i^{m\times n\times c} \mathrm{SimVec}(i)}{m \times n \times c} \mathrm{mod1}, \tag{11}$$

$$x_u = \frac{x_0 + \delta}{2}. \tag{12}$$

(7) Apply Chebyshev mapping using x_u and B for $m \times n \times c$ times to produce a sequence X.

(8) Add the elements of sequence X to the elements of sequence ReP to obtain sequence R as follows:

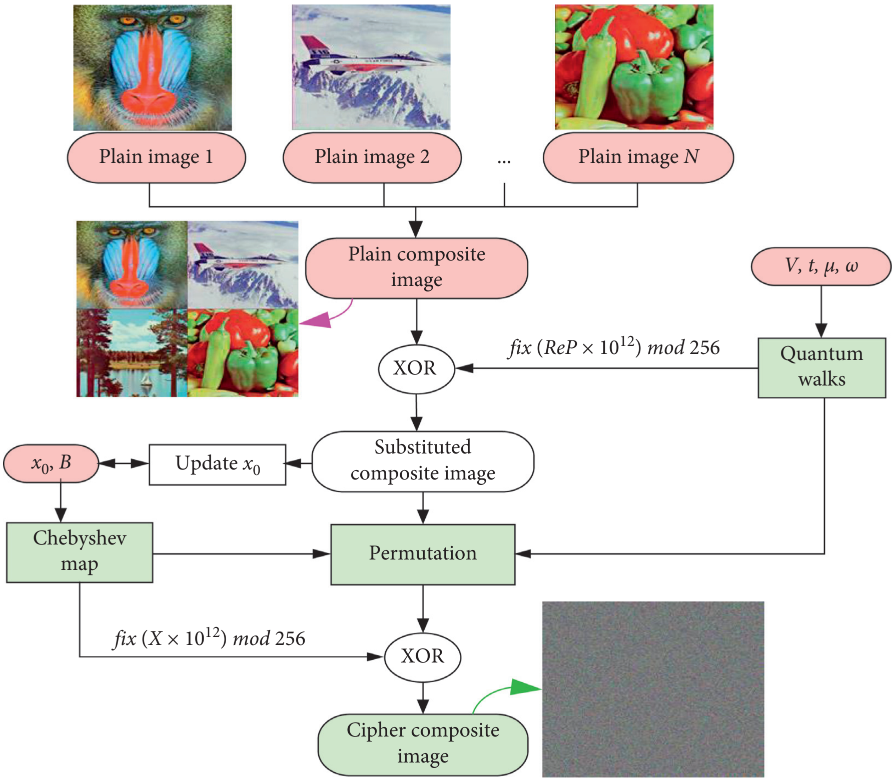


Figure 1: Outline of encryption procedure for the proposed multiple-image cryptosystem.

$$R_k = X_k + \operatorname{Re} P_k, \quad \text{for } k = 1, 2, \ldots, m \times n \times c. \tag{13}$$

(9) Arrange the elements of R in ascending order as RA and retrieve the index of each element of RA in R as PerVec.

(10) Permutate the substituted composite image SimVec using the generated PerVec such that

$$\operatorname{PerIm}(k) = \operatorname{SimVec}(\operatorname{PerVec}(k)), \quad \text{for } k = 1, 2, \ldots, m \times n \times c. \tag{14}$$

(11) Obtain the key sequence (Key2) by transforming the sequence X into integer values.

$$\text{Key2} = \operatorname{fix}\left(X \times 10^{12}\right)\text{mod256}. \tag{15}$$

(12) Execute Bitwise XOR process on the permutated composite image PerIm and key2 to obtain the cipher composite image Cim as

$$\begin{aligned} \text{CimVec} &= \text{PerIm} \oplus \text{Key2}, \\ \text{Cim} &= \operatorname{reshape}(\text{CimVec}, m, n, c). \end{aligned} \tag{16}$$

3.2. Decryption Algorithm. The decryption method (Figure 2) of the proposed cryptosystem is the reverse process of the encryption process, and it is executed in the steps enumerated as follows:

(1) Convert the cipher composite image Cim into a vector CimVec.

(2) Use the primary key parameters (x_0, B) for the Chebyshev map to update the initial key parameter x_0 using δ.

$$x_u = \frac{x_0 + \delta}{2}. \tag{17}$$

(3) Apply Chebyshev mapping using x_u and B for $m \times n \times c$ times to produce a sequence X.

(4) Obtain the key sequence (DKey1) by converting the sequence X into integer values.

$$\text{DKey1} = \operatorname{fix}\left(X \times 10^{12}\right)\text{mod256}. \tag{18}$$

(5) Execute Bitwise XOR operation on CimVec and DKey1 to obtain the permutated composite image PerIm.

(6) Use the primary key parameters (V, t, μ, ω) for operating QWs t times on a cycle of odd V nodes to produce a probability distribution P of size V.

(7) Resize P to the dimension of the composite image CimVec ($m \times n \times c$).

$$\operatorname{Re} P = \operatorname{resize}(P, [\, m \times n \times c \quad 1 \,]). \tag{19}$$

(8) Add the elements of sequence X to the elements of sequence ReP to obtain sequence R.

(9) Arrange the elements of R in ascending order (as RA) and retrieve the index of each element of RA in R as DPerVec.

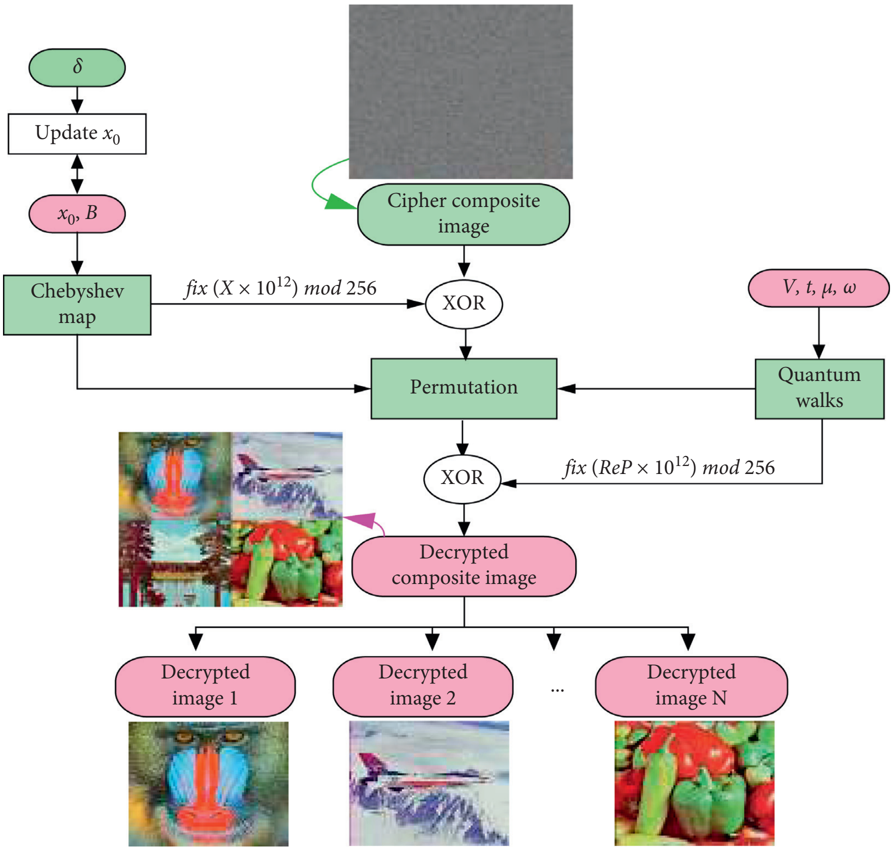


Figure 2: Structure of the decryption procedure for the proposed multiple-image cryptosystem.

(10) Rearrange (or depermutate) the permutated composite image PerIm using the generated DPerVec such that

$$\mathrm{DPerIm}(\mathrm{DPerVec}(k)) = \mathrm{PerIm}(k), \quad \text{for } k = 1, 2, \ldots, m \times n \times c. \tag{20}$$

(11) Obtain the key sequence (DKey2) via conversion of ReP into integer values.

$$\mathrm{DKey2} = \mathrm{fix}\left(\mathrm{Re}\,P \times 10^{12}\right)\mathrm{mod}256. \tag{21}$$

(12) Execute the Bitwise XOR operation process on the depermutated composite image DPerIm and DKey2 to obtain the DimVec and decrypted composite image DecIm as

$$\begin{gathered}\mathrm{DimVec} = \mathrm{DPerIm} \oplus \mathrm{DKey2},\\ \mathrm{DecIm} = \mathrm{reshape}(\mathrm{DimVec}, m, n, c).\end{gathered} \tag{22}$$

(13) Decomposite the decrypted composite image DecIm to get the decrypted images (DIg01, DIg02, . . ., DIg0N).

4. Experimental Validation

To appraise the performance of the proposed multi-image cryptosystem, experiments executed using a laptop with Intel Core™ i5-2450M, 6 GB RAM and implemented using MATLAB R2016b are reported in this section. The dataset used are sourced from the Signal and Image Processing Institute (SIPI) database in [32]. Four images each of size 512 × 512 and labelled as Ig01 through Ig04 (see Figure 3) were selected and used for the experiments.

Whereas the initial values for key parameters (i.e., V, t, μ, ω, x_0, and B) can be selected according to their ranges, in this study, the used initial parameter settings for running the QWs are set as $V = 301$, $t = 325$, $\mu = 0$, and $\omega = \pi/6$. Similarly, initial parameter settings for iterating the Chebyshev map are set as $x_0 = 0.6743$ and $B = 55$. Figure 4 presents the plain composite image consisting of input images Ig01 (Baboon), Ig02 (Airplane), Ig03 (Boat), and Ig04 (Peppers) as well as the resulting cipher composite image obtained using our multi-image cryptosystem and the decrypted composite image obtained using our multi-image cryptosystem for the provided initial key parameters. To guarantee the effectiveness of our cryptosystem, in addition to the composite images, we analysed the properties of the input images (Ig01, Ig02, Ig03, and Ig04) and their respective decomposed cipher composite image versions (Cipher-Ig01, Cipher-Ig02, Cipher-Ig03, and Cipher-Ig04) as presented in Figure 5.

The remainder of this section presents an extensive analysis of our proposed scheme using the dataset introduced earlier (in Figure 3). However, throughout the ensuing discussion and performance evaluation, we shall refer to the pristine or unadulterated input images (i.e., Ig01, Ig02, Ig03, and Ig04 and their composite image) as

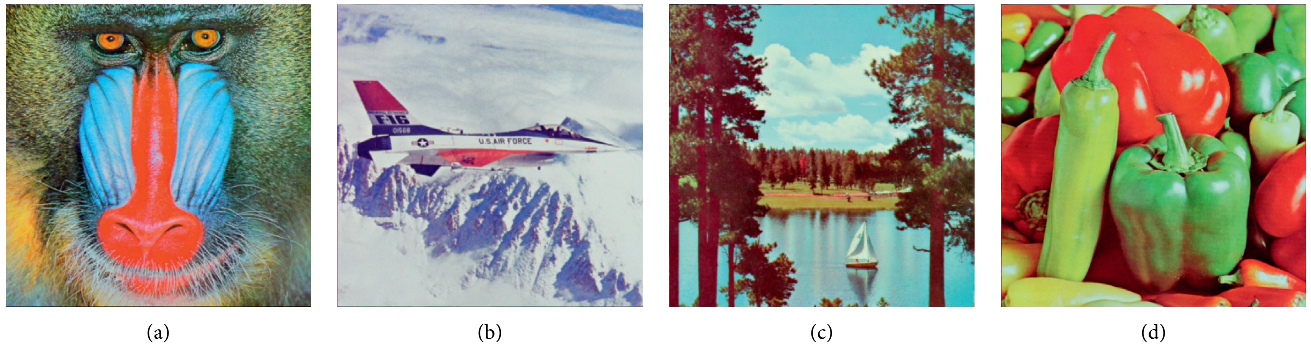

(a) (b) (c) (d)

Figure 3: Sub-dataset used as input images (sourced from [32]) to validate the proposed cryptosystem. (a) Ig01. (b) Ig02. (c) Ig03. (d) Ig04.

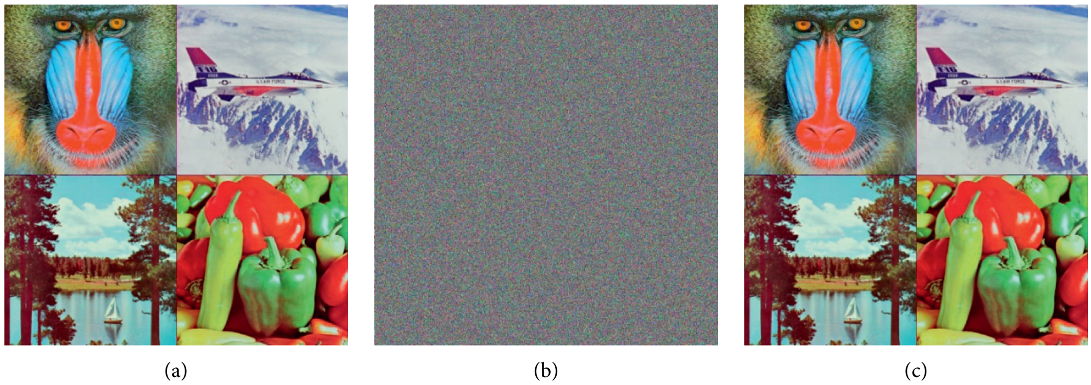

(a) (b) (c)

Figure 4: (a) Plain composite image (which consists of input images Ig01, Ig02, Ig03, and Ig04), (b) the cipher composite image obtained using our proposed multiple-image cryptosystem, and (c) the decrypted composite image.

the pristine group whilst their corresponding ciphered versions are collectively referred to as the cipher group.

4.1. Correlation Analysis. To assess the concordance between neighbouring pixels X and Y in an image, we use correlation coefficient, Corr, where it is established that pristine (i.e., unadulterated) images exhibit correlation values near 1 in each direction and that of a cipher image from a well-designed cryptosystem should be close to 0 [27]. To calculate the correlation coefficients for our multiple-image cryptosystem, we picked 10^4 pairs of neighbouring pixels per direction at random and *Corr* is computed using

$$\mathrm{Corr} = \frac{\sum_{k=1}^{N}\left(a_k - \overline{a}\right)\left(b_k - \overline{b}\right)}{\sqrt{\sum_{k=1}^{N}\left(a_k - \overline{a}\right)^2 \sum_{k=1}^{N}\left(b_k - \overline{b}\right)^2}}, \qquad (23)$$

where a_k, and b_k are the values of the two adjacent pixel values, and N denotes the total number of adjacent pixel pairs per direction.

Table 1 presents the outcomes of the correlation coefficient test, where we see that the correlation coefficient values of the cipher images are close to 0. Similarly, the correlation distributions for the red, blue, and green channels of the composite image are presented in Figures 6–8, respectively. It is apparent from these outcomes that no intelligible information about the composite image can be obtained from the figures.

4.2. Histogram Analysis. Histogram analysis is a widely used image evaluation that reflects the frequency distribution of pixels in an image [27]. A well-designed cryptosystem should produce ciphers with uniformly distributed histogram. Figure 9 presents the histograms of the plain composite image and its corresponding cipher composite image. From these plots, we can deduce that the distributions of the plain composite image are markedly different for each channel whilst those for the ciphered composite image have flat histograms, which indicates the absence of useful information. Furthermore, we employ the chi-square measure (χ^2) to quantify the pixel distribution in the histograms as defined in

$$\chi^2 = \sum_{k=0}^{255} \frac{\left(f_k - N\right)^2}{N}, \qquad (24)$$

where f_k is the pixel value with frequency k, and N is the dimension of the image.

It is instructive that by assuming a significant level $\alpha = 0.05$, then for the maximum greyscale value $\chi^2(255) = 293.3$. Therefore, an image with χ^2 less than $\chi^2(255)$ has a uniform pixel distribution. Otherwise, the histogram is considered nonuniformly distributed. Based on this, Table 2 presents results of the χ^2 test for our pristine and cipher groups, respectively. The outcomes show that all images in the cipher group have χ^2 values less than the threshold value of 293.3, which conforms with the flat-out plots of their histograms presented earlier in

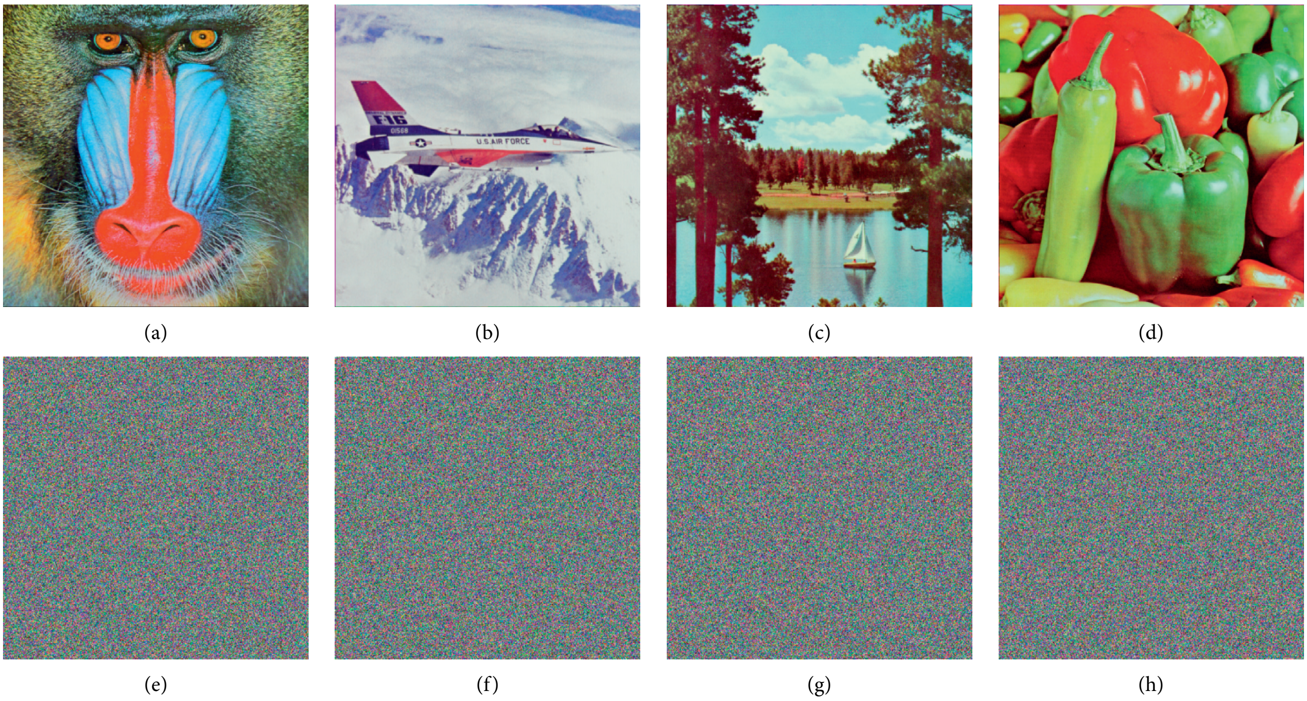


Figure 5: Pristine (or input) images (a) Ig01, (b) Ig02, (c) Ig03, and (d) Ig04 and their respective ciphered versions (e) Cipher-Ig01, (f) Cipher-Ig02, (g) Cipher-Ig03, and (h) Cipher-Ig04.

Table 1: Correlation coefficient test for the pristine and cipher groups for input and composite images.

Group	Image	Colour component	Direction		
			Horizontal	Vertical	Diagonal
Pristine	Plain composite	R	0.9280	0.9527	0.9189
		G	0.9501	0.9617	0.9312
		B	0.9614	0.9695	0.9476
Cipher	Cipher composite	R	−0.0005	0.0002	−0.0009
		G	−0.0001	−0.0003	0.0009
		B	−0.0002	−0.0005	−0.0001
Pristine	Ig01	R	0.8678	0.9196	0.8574
		G	0.7709	0.8649	0.7464
		B	0.8843	0.9081	0.8389
Cipher	Cipher-Ig01	R	0.0006	0.0002	0.0006
		G	−0.0006	−0.0007	0.0002
		B	−0.0005	−0.0001	0.0005
Pristine	Ig02	R	0.9651	0.9726	0.9412
		G	0.9679	0.9630	0.9382
		B	0.9534	0.9613	0.9336
Cipher	Cipher-Ig02	R	0.0001	0.0008	−0.0009
		G	−0.0009	−0.0007	0.0009
		B	−0.0003	0.0005	0.0003
Pristine	Ig03	R	0.9542	0.9542	0.9427
		G	0.9657	0.9725	0.9533
		B	0.9729	0.9713	0.9562
Cipher	Cipher-Ig03	R	0.0008	−0.0008	−0.0001
		G	0.0007	0.0009	0.0007
		B	−0.0007	−0.0007	−0.0004
Pristine	Ig04	R	0.9657	0.9647	0.9590
		G	0.9856	0.9837	0.9750
		B	0.9696	0.9660	0.9505
Cipher	Cipher-Ig04	R	−0.0009	0.0006	−0.0006
		G	0.0009	−0.0005	−0.0007
		B	−0.0002	−0.0001	−0.0001
Average values for cipher group			−0.00012	−0.00008	0.00002

Figure 9. Hence, it can be concluded that our multiple-image cryptosystem can withstand histogram-based attacks.

4.3. Entropy Analysis. Information entropy $E(X)$ is a test used to compute the concentration of pixel values per bit-level in an image $E(X)$. It is considered a measure of efficiency of a cryptosystem [27], and it can be computed using

$$E(X) = \sum_{k=0}^{255} p(x_k)\log_2 \frac{1}{p(x_k)}, \tag{25}$$

where $p(x_k)$ indicates the probability of x_k.

Theoretically, grey scale images with 2^8 values should have an optimal entropy of 8 bits. In other words, when efficiently ciphered, such an image should have an entropy value close to 8. However, this global entropy does not consider the apparent randomness in such ciphered images, which motivates the use of a modified or local entropy measure is used to atone for the randomness. The local entropy is the average values of global entropy in non-overlapping blocks (i.e., 1936 pixels within the block).

Like in the global entropy, values of local entropy closer to 8 are indications of an efficient cryptosystem. Table 3 presents a summary of local and global entropies for the pristine and cipher groups of our performance analysis. As deduced from the table, all global entropies for the cipher group are within a difference of 0.0002 from the expected value of 8, which validates the efficiency of our proposed scheme in terms of its ability to withstand different entropy-based attacks.

4.4. Differential Test. In addition to performing creditably in the statistical tests, a well-designed cryptosystem should exhibit sensitivity to tiny modifications in the composition of its pristine version. In this study, we utilise two measures: the number of pixels change rate (NPCR) and unified average changing intensity (UACI) defined in equations (26) and (27) for the differential test [33] to assess these modifications.

$$\mathrm{NPCR}(C1, C2) = \frac{\sum_{i;j} Df(i,j)}{T} \times 100\%,$$
$$Df(i,j) = \begin{cases} 0, & \text{if } C1(i,j) = C2(i,j), \\ 1, & \text{if } C1(i,j) \neq C2(i,j), \end{cases} \tag{26}$$

$$\mathrm{UACI}(C1, C2) = \frac{1}{T}\left(\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255}\right) \times 100\%, \tag{27}$$

where T is the total pixels within the image, while $C1$ and $C2$ are cipher composite images for a pristine (i.e., original or plane) composite image with just one bit modified.

Computations of the NPCR and UACI (in %) when making tiny modifications in pixel value at position (1, 1) from 164 to 165 of the red channel of the pristine composite image are presented in Table 4. Theoretically, for an image to be considered uniformly distributed, its respective NPCR and UACI values should be as close to 99.6% and 33.33% as possible.

Results reported in Table 4 show that, on average, our proposed scheme is within 0.01% and 0.1% of the expected ranges of the NPCR and UACI, respectively, which validates its capability to in withstand differential attacks.

4.5. Contrast Test. Contrast analysis (T) is a statistical measure used to assess the local intensity variation in an image. T can be defined as presented in the following equation [34]:

$$T = \sum_{i,j} |i - j|^2 p(i,j), \tag{28}$$

where $p(i, j)$ indicates the number of grey level co-occurrence matrices.

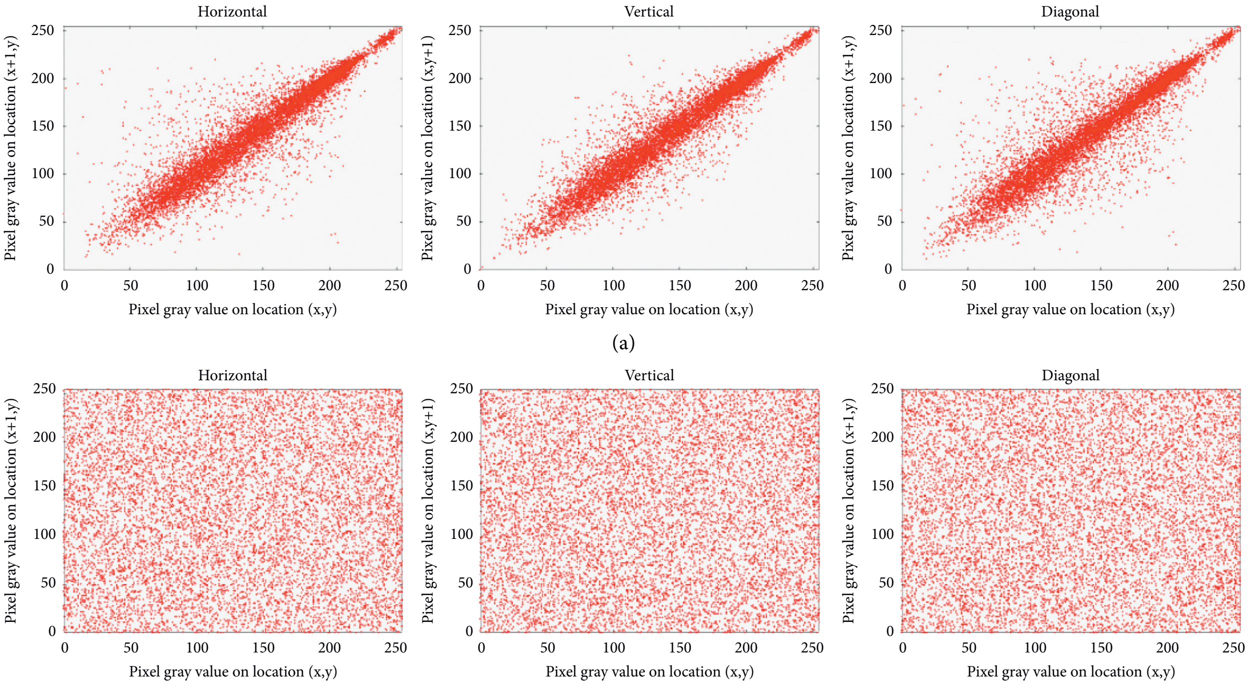
Given an image, high contrast values signify presence of significantly distinct grey levels while lower values indicate constant grey levels. The outcomes of the contrast test presented in Table 5 show that the cipher images obtained from our scheme exhibit higher contrast values relative to their corresponding pristine versions.

4.6. Key Sensitivity Test. A robustly efficient cryptosystem should show sensitivity to changes in the composition of its secret key. In other words, to withstand attacks, such as brute-force attacks, an efficient cryptosystem must be sensitive to alterations to its secret key parameters.

To analyse the key sensitivity of our proposed scheme, we considered recovery (i.e., decryption) of the ciphered composite image (in Figure 4(b)) for different modifications in the secret key parameters. The outcomes of this key sensitivity analysis are presented in Figure 10 for changes in V, T, μ, ω, x_0, and B, respectively. As manifested in these outcomes, for each modification, the pristine composite image is unrecovered.

Furthermore, by pairing the decrypted cipher image (i.e., in Figure 4(c)) with the decrypted images for slight modifications in secret key parameters (i.e., in Figure 10) and computing their respective pixel difference rate, namely, pairing of the targeted decrypted composite image with those for different alternations in key parameters, we establish the quantitative performance of the key sensitivity of our scheme. Results of our pixel difference rate (in %) are presented in Table 6 and outcomes therein suggest that, despite the slight changes in key parameters, a high pixel difference rate is high (approximately 99.61%) is maintained throughout. Furthermore, the recovered images are composed of unintelligible noise and the recovered images remain incongruous. This is a testimony of our proposed scheme's sensitivity to alterations to the composition of its secret key parameters.

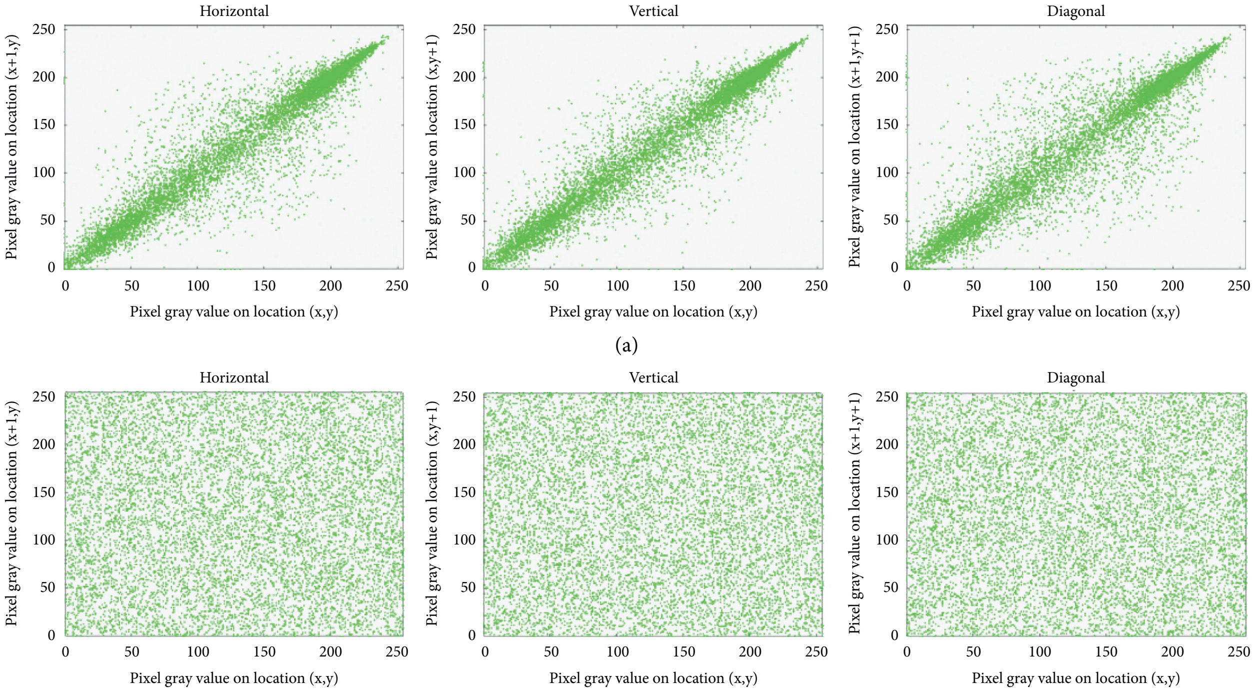
4.7. Noise and Occlusion Attacks. In the course of its transmission over different communication networks, data can be tampered, lost, or violated. Consequently, an efficient



(a)

(b)

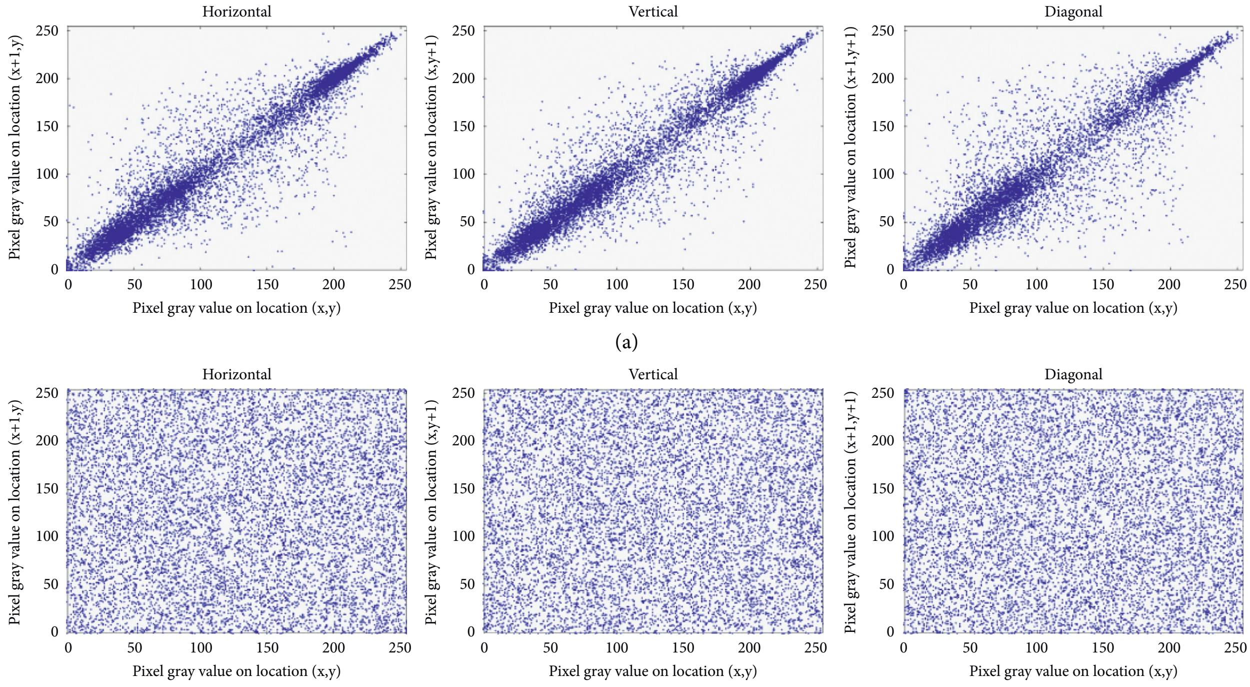
Figure 6: Correlation distribution for red component of plain composite image in Figure 4(a) (a) and those from the cipher composite image in Figure 4(b) (b).



(a)

(b)

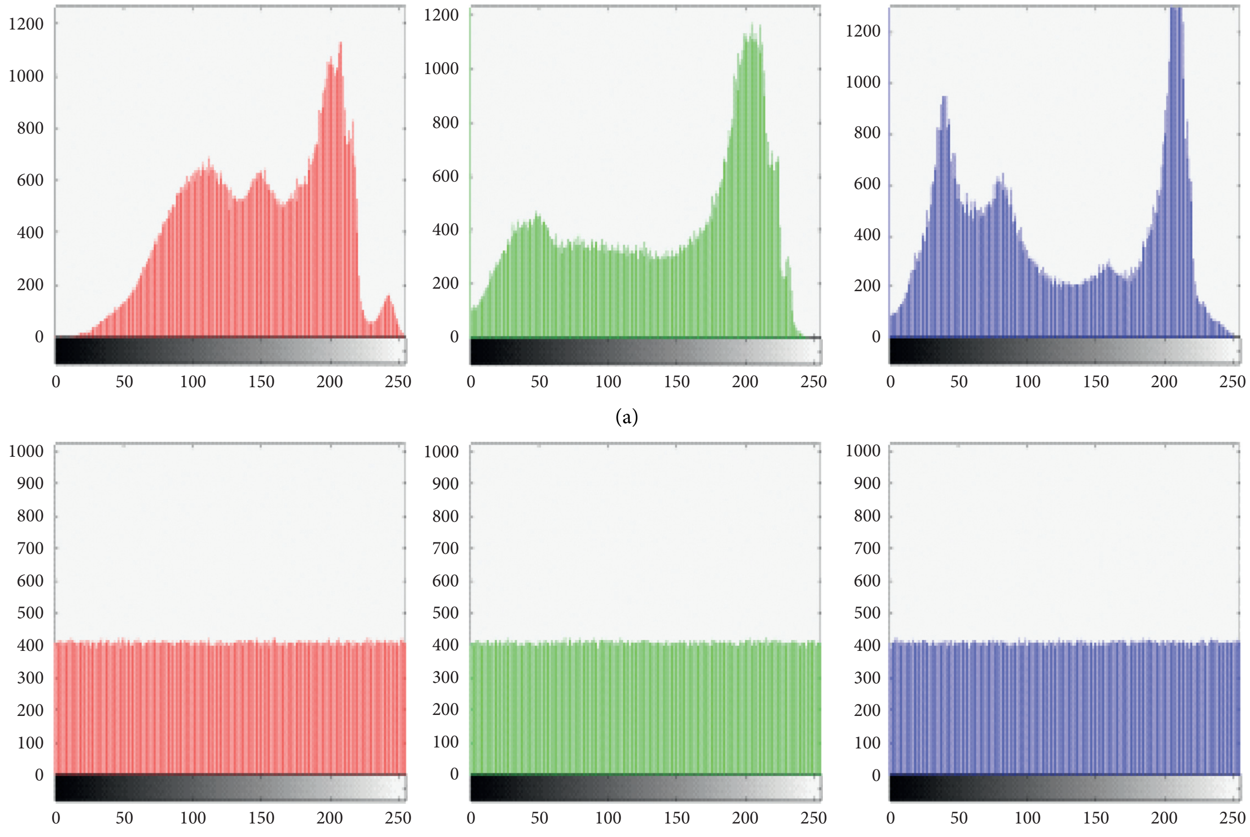
Figure 7: Correlation distribution for green component of plain composite image in Figure 4(a) (a) and those from the cipher composite image in Figure 4(b) (b).



(a)

(b)

Figure 8: Correlation distribution for blue component of plain composite image in Figure 4(a) (a) and those from the cipher composite image in Figure 4(b) (b).



(a)

(b)

Figure 9: Histogram distribution for plain composite image in Figure 4(a) (a) and the cipher composite image in Figure 4(b) (b).

Table 2: Chi-square values for images in the pristine and cipher groups.

Image	Pristine group			Cipher group		
	R	*G*	*B*	*R*	*G*	*B*
Composite image	561115.509	466430.302	648823.932	228.317	224.622	208.914
Ig01	82839.728	142808.039	79942.617	245.619	236.990	219.396
Ig02	678424.492	682495.382	1107858.005	238.957	265.861	272.330
Ig03	196697.306	130154.716	344571.537	264.919	259.925	218.814
Ig04	213187.216	318382.929	491428.177	225.269	252.263	209.951
Average values	346452.850	348054.274	534524.854	240.616	247.932	225.881

Table 3: Local and global information entropies of the studied dataset.

Image	Local entropy		Global entropy	
	Pristine group	Cipher group	Pristine group	Cipher group
Composite image	6.07368	7.90167	7.72801	7.99995
Ig01	6.64443	7.90172	7.76243	7.99978
Ig02	5.52864	7.90234	6.66391	7.99975
Ig03	6.07741	7.90257	7.76216	7.99979
Ig04	6.04964	7.90193	7.66982	7.99978
Average values	6.07476	7.90205	7.51727	7.99981

Table 4: Outcomes of NPCR and UACI for slight changes in the pristine composite image.

Group	Image	NPCR (%)	UACI (%)
Pristine	Composite image	99.60543	33.45229
	Ig01	99.60645	33.42891
	Ig02	99.60058	33.46614
	Ig03	99.60467	33.45160
	Ig04	99.61102	33.46251
Average values		99.60563	33.45229

cryptosystem should be designed to curtail such attacks. To assess the ability of our proposed scheme to withstanding the enumerated violations, we report outcomes of noise and occlusion attacks.

For the noise attacks, we considered the impact of using Salt and Pepper (S&N) noise to tamper with the ciphered composite image in Figure 4(b). For effective analysis, the density of S&N noise was varied as 0.1, 0.15, and 0.25; outcomes for which are presented in Figures 11(a)–11(c), respectively. Figures 11(d)–11(f) present the recovered versions of the respective images.

Similarly, the occlusion attacks were assessed for different cut-outs occluding the parts of the same ciphered composite in Figure 4(b). The cut-out size was varied to cover 10%, 25%, and 35% of the ciphered image as presented in Figures 12(a)–12(c), while the recovered versions of these images are presented in Figures 12(d)–12(f).

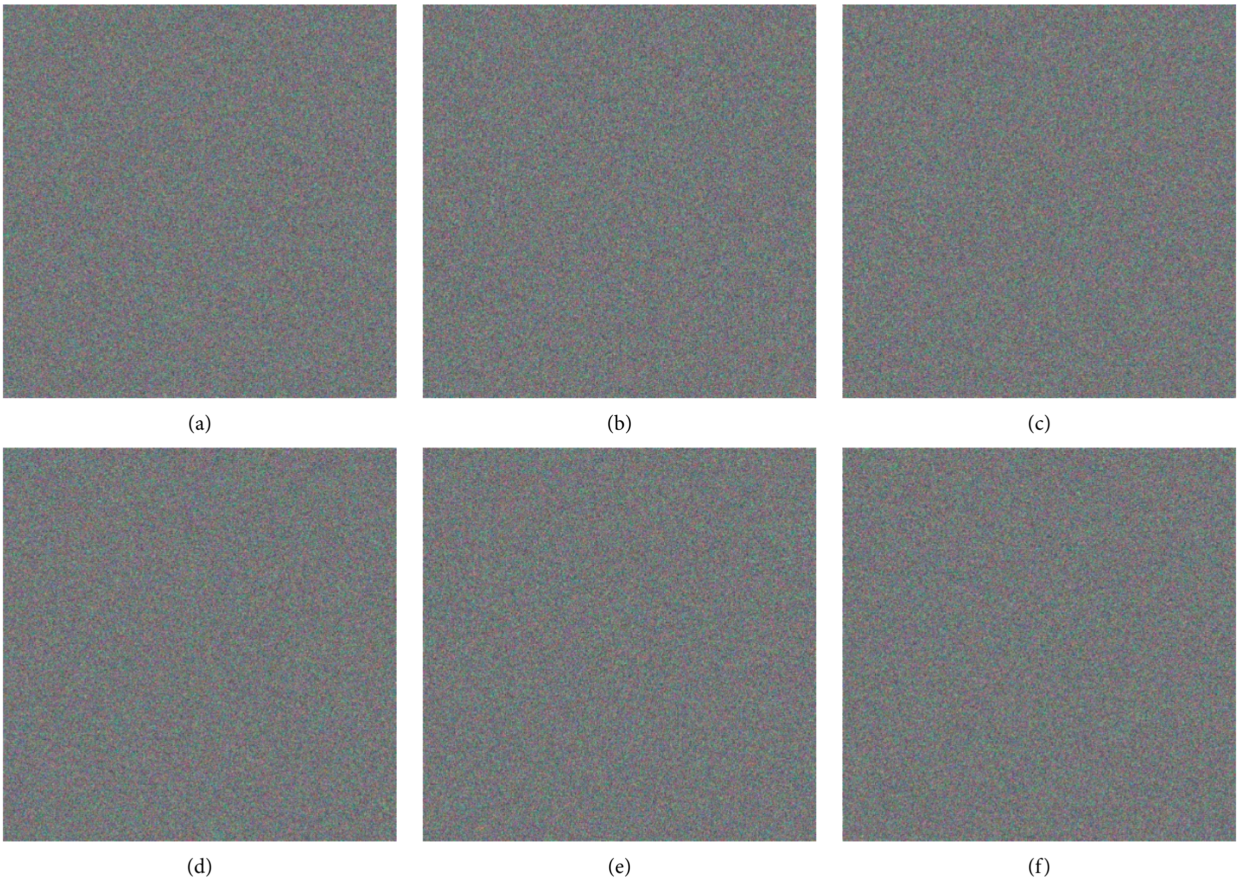
In both analyses, we note the ability to recover clear versions of the input composite image despite the noise and occlusion attacks. This validates the ability of our proposed scheme to overcome such prevalent attacks.

4.8. Randomness Analysis. To validate the randomness of the constructed cipher composite image, the NIST SP 800-22 tests [35] were executed. The main goal of these tests is to detect any nonrandomness property in the constructed cipher composite image. These tests are executed on a sequence of 10^6 bits from the cipher composite image whose outcomes are presented in Table 7. It is apparent from these outcomes that the constructed cipher composite image obtained using the proposed cryptosystem is completely random.

4.9. Comparative Analysis. To establish the effectiveness of our proposed multi-image cryptosystem, we compare our results alongside those from other chaotic cryptosystems. Results reported in Table 8 show the average values of correlation coefficients UACI, NPCR, and global entropy for our cryptosystem and those indicated in the table. From these outcomes, it is apparent from these outcomes that the proposed scheme is effective and reliable for various cryptographic applications.

Table 5: Contrast values of the investigated dataset.

Image	Pristine group			Cipher group		
	R	*G*	*B*	*R*	*G*	*B*
Composite image	0.349001	0.470013	0.427496	10.540164	10.486821	10.507776
Ig01	0.615911	0.762479	0.849334	10.501574	10.491029	10.519275
Ig02	0.184736	0.285026	0.133359	10.541669	10.487719	10.497809
Ig03	0.294325	0.486102	0.461583	10.536192	10.451294	10.496693
Ig04	0.275149	0.302998	0.221375	10.583426	10.517864	10.519198
Average values	0.343824	0.461324	0.418629	10.540605	10.486945	10.508150



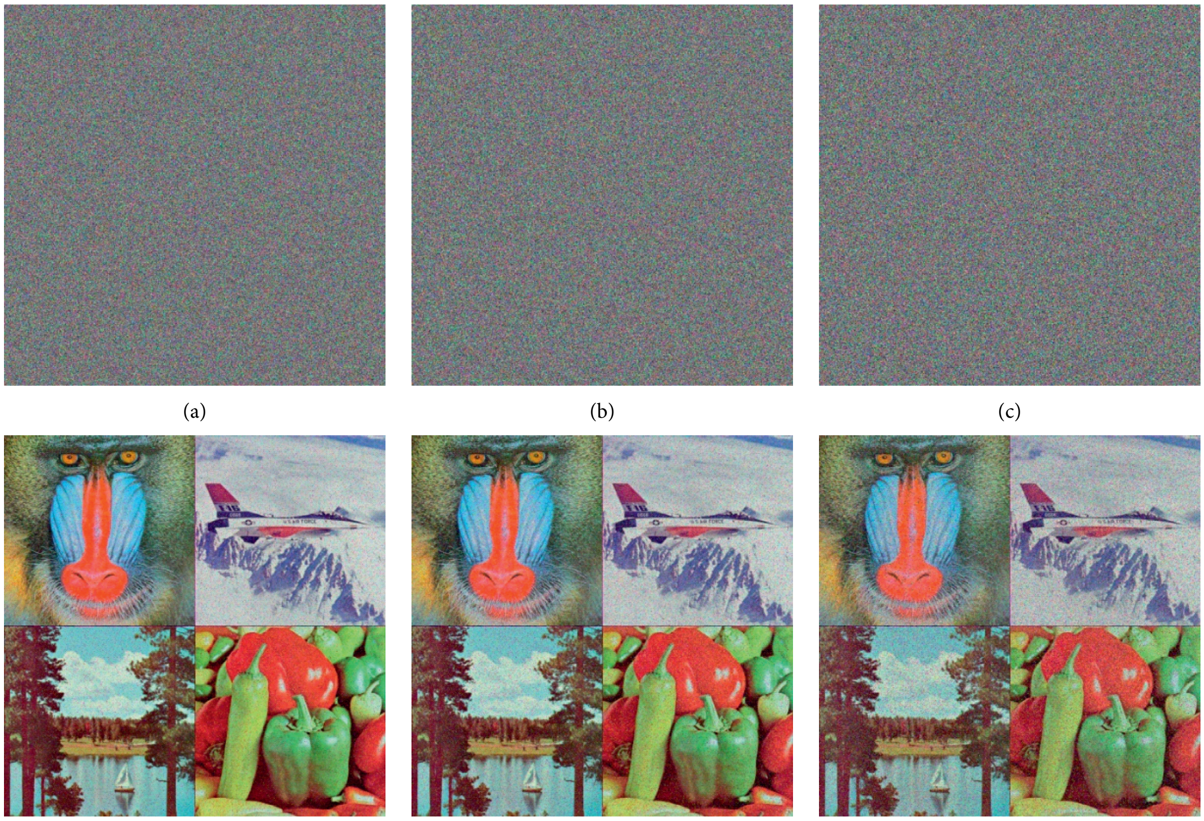
(a) (b) (c)

(d) (e) (f)

Figure 10: Decryption process for the cipher composite image (Figure 4(b)) for different alterations to secret key parameters. (a) Actual key with alteration at $V = 303$. (b) Actual key with alteration at $t = 324$. (c) Actual key with alteration at $\mu = \pi/2$. (d) Actual key with alteration at $\omega = \pi/3$. (e) Actual key with alteration at $x_0 = 0.674300000000001$. (f) Actual key with alteration at $B = 56$.

Table 6: Pixel difference rate for pairings of decrypted composite image (i.e., using the actual key parameters (in Figure 4(c)) and those decrypted using different alterations in secret key parameters (Figures 10(a)–10(f)).

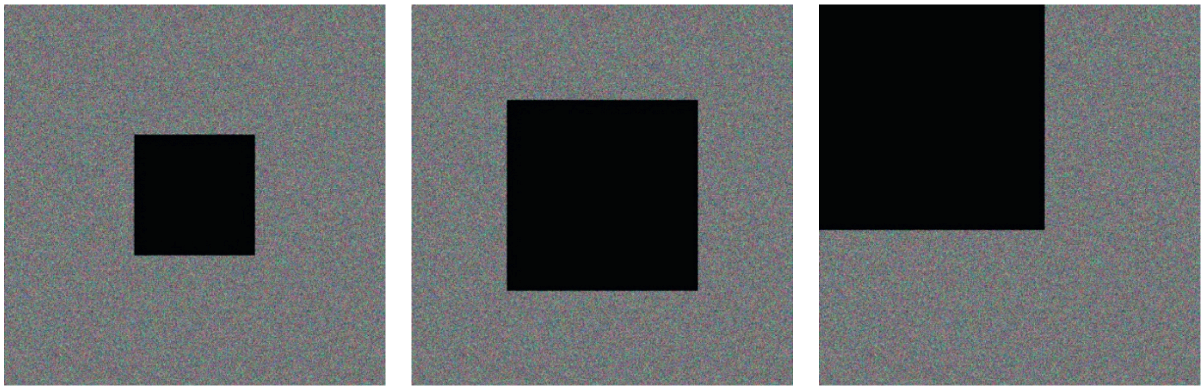
Image pairing	Difference rate (%)
Figures 10(a) and 4(c)	99.61503
Figures 10(b) and 4(c)	99.60962
Figures 10(c) and 4(c)	99.60887
Figures 10(d) and 4(c)	99.60924
Figures 10(e) and 4(c)	99.61376
Figures 10(f) and 4(c)	99.61058
Average values	99.61118



(a) (b) (c)

(d) (e) (f)

Figure 11: Noise attack. (a–c) Ciphered version of composite image (Figure 4(b)) with S&N noise of varying densities (i.e., 0.1, 0.15, and 0.25) added. (d–f) Recovered versions of the corrupted images.



(a) (b) (c)

Figure 12: Continued.

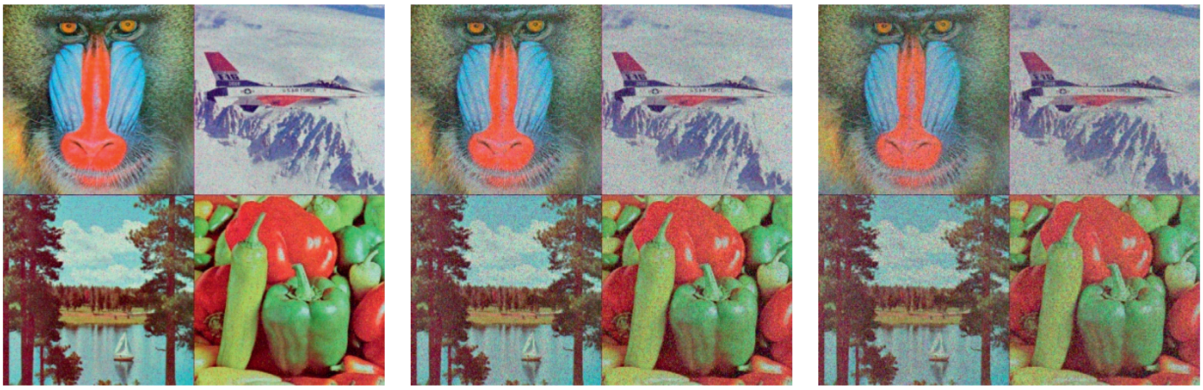


Figure 12: Occlusion attacks. (a–c) Ciphered version of composite image (Figure 4(b)) with cut-out occlusions covering 10%, 25%, and 25% of its content. (d–f) Recovered versions of the occluded images.

Table 7: Outcomes of randomness test for the cipher composite image (Figure 4(b)).

Test		P value	Outcome
Overlapping templates		0.860314	Passed
Approximate entropy		0.094379	Passed
DFT		0.349265	Passed
Nonoverlapping templates		0.399560	Passed
Block frequency		0.673566	Passed
Universal		0.672334	Passed
Runs		0.110948	Passed
Random excursions		0.357085	Passed
Long runs of ones		0.890293	Passed
Frequency		0.819646	Passed
Random excursions variant		0.137987	Passed
Rank		0.933441	Passed
Linear complexity		0.292944	Passed
Serial	Test 1	0.325773	Passed
	Test 2	0.685080	Passed
Cumulative sums	Forward	0.914406	Passed
	Reverse	0.718627	Passed

Table 8: Comparison of proposed cryptosystem alongside other chaos-based multi-image cryptosystems.

Cryptosystem	NPCR (%)	UACI (%)	Correlation			Global entropy
			H	V	D	
Proposed	99.6056	33.4523	−0.00012	−0.00008	0.00002	7.9998
[14]	99.6131	33.4660	−0.00364	0.00262	0.00124	7.9995
[16]	30.5379	99.5977	0.00530	−0.00600	−0.02300	7.9961
[17]	99.6743	33.5358	0.00281	0.00046	0.00049	7.9995
[18]	99.6200	33.5000	−0.00115	0.00173	0.00413	7.9993
[19]	99.6225	33.4375	−0.00223	−0.00248	0.00158	7.9993

5. Concluding Remarks

Exploiting the stochastic transitions between states, and randomness attributed to quantum walks on the one side and the semigroup membership and chaos of Chebyshev map on the other, our study proposes an efficient multi-image cryptosystem that exhibits nonlinear chaotic dynamic behaviours. Simulation results prove that the proposed cryptosystem is effective and reliable across wide-range cryptographic applications.

Besides the merits ascribed to traditional chaos systems, our cryptosystem is an excellent tool to generate efficient encryption keys, espouse high sensitivity to initial and system parameters, manifest good unpredictability, pseudorandomness, stability, periodicity, and infinite key space needed to efficiently resist brute-force attacks.

In addition to designing reliable multi-image cryptosystems, a major objective of this study is advancing studies to integrate quantum computing models with digital computing models for designing reliable cryptosystems. Currently and in the future, we intend to extend this work towards designing new secret-sharing cryptosystems.

Data Availability

The datasets generated and analysed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this study and its contents.

Acknowledgments

This study was sponsored by the Prince Sattam bin Abdulaziz University, Saudi Arabia, via the Deanship for Scientific Research funding for the Advanced Computational Intelligence and Intelligent Systems Engineering (ACIISE) Research Group (Project no. 2020/01/12173).

References

[1] "Bernard marr—intelligent business performance," 2021, https://www.bernardmarr.com.

[2] "How many photos will be taken in 2021?—mylio blog, ," vol. 1, 2021, https://blog.mylio.com/how-many-photos-will-be-taken-in-2021/.

[3] J. Socolar, *Chaos, Encyclopedia of Physical Science and Technology*, Elsevier, Amsterdam, Netherlands, Third edition, 2003.

[4] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, "Analytic study of a novel color image encryption method based on the chaos system and color codes," *Complexity*, vol. 2021, Article ID 5499538, 19 pages, 2021.

[5] X. Li, Z. Xie, J. Wu, and T. Li, "Image encryption based on dynamic filtering and bit cuboid operations," *Complexity*, vol. 2019, Article ID 7485621, 18 pages, 2019.

[6] Z. Li, C. Peng, W. Tan, and L. Li, "An effective chaos-based image encryption scheme using imitating jigsaw method," *Complexity*, vol. 2021, Article ID 8824915, 18 pages, 2021.

[7] 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 Computing & Applications*, vol. 31, no. 11, pp. 7111–7130, 2019.

[8] T. Yan and D. Li, "A novel color image encryption scheme based on controlled alternate quantum walks and DNA sequence operations," *Machine Learning for Cyber Security*, Springer, Cham, Germany, pp. 297–306, 2020.

[9] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, "An image encryption approach using particle swarm optimization and chaotic map," *International Journal of Information Technology*, vol. 10, no. 3, pp. 247–255, 2018.

[10] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dynamics*, vol. 100, no. 1, pp. 699–711, 2020.

[11] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[12] K. A. K. Patro and B. Acharya, "An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system," *Nonlinear Dynamics*, vol. 104, pp. 2759–2805, 2021.

[13] Z. Shao, X. Liu, Q. Yao, N. Qi, Y. Shang, and J. Zhang, "Multiple-image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyrator domain," *Signal Processing: Image Communication*, vol. 80, Article ID 115662, 2020.

[14] M. Zarebnia, H. Pakmanesh, and R. Parvaz, "A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images," *Optik*, vol. 179, pp. 761–773, 2019.

[15] C.-L. Li, H.-M. Li, F.-D. Li, D.-Q. Wei, X.-B. Yang, and J. Zhang, "Multiple-image encryption by using robust chaotic map in wavelet transform domain," *Optik*, vol. 171, pp. 277–286, 2018.

[16] A. Bisht, M. Dua, and S. Dua, "A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 9, pp. 3519–3531, 2019.

[17] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps," *Mathematics and Computers in Simulation*, vol. 178, pp. 646–666, 2020.

[18] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and permutation," *Optics and Lasers in Engineering*, vol. 92, pp. 6–16, 2017.

[19] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7841–7869, 2019.

[20] B. Abd-El-Atty, A. M. Iliyasu, A. Alanezi, and A. A. Abd Ellatif, "Optical image encryption based on quantum walks," *Optics and Lasers in Engineering*, vol. 138, Article ID 106403, 2021.

[21] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in iot-based smart cities," *Information Processing & Management*, vol. 58, no. 4, Article ID 102549, 2021.

[22] S. E. Venegas-Andraca, "Quantum walks: a comprehensive review," *Quantum Information Processing*, vol. 11, no. 5, pp. 1015–1106, 2012.

[23] C. Vlachou, J. Rodrigues, P. Mateus, N. Paunković, and A. Souto, "Quantum walk public-key cryptographic system," *International Journal of Quantum Information*, vol. 13, no. 7, Article ID 1550050, 2015.

[24] D. Nguyen, D. Nolan, and N. Borrelli, "Quantum walks in quasi-periodic photonics lattices," in *Proceedings of the 2019 IEEE Photonics Society Summer Topical Meeting Series (SUM)*, pp. 1-2, IEEE, Ft. Lauderdale, FL, USA, July 2019.

[25] Y. G. Yang, Q. X. Pan, S. J. Sun, and P. Xu, "Novel image encryption based on quantum walks," *Scientific Reports*, vol. 5, no. 1, pp. 7784–7789, 2015.

[26] J. Shi, H. Chen, F. Zhou, L. Huang, S. Chen, and R. Shi, "Quantum blind signature scheme with cluster states based on quantum walk cryptosystem," *International Journal of Theoretical Physics*, vol. 58, no. 4, pp. 1337–1349, 2019.

[27] A. A. Abd El-Latif, B. Abd-el-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time

quantum walks with induced chaotic dynamics and cryptographic applications," *Scientific Reports*, vol. 10, no. 1, pp. 1–16, 2020.

[28] J. Julian Rosen, Z. Zachary Scherr, B. Benjamin Weiss, and E. Z. Michael, "Chebyshev mappings of finite fields," *The American Mathematical Monthly*, vol. 119, no. 2, pp. 151–155, 2012.

[29] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman, "Exponential algorithmic speedup by a quantum walk," in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pp. 59–68, San Diego, CA, USA, June 2003.

[30] T. Kohda, A. Tsuneda, and A. J. Lawrance, "Correlational properties of chebyshev chaotic sequences," *Journal of Time Series Analysis*, vol. 21, no. 2, pp. 181–191, 2000.

[31] "Bicubic interpolation resize procedure," 2021, https://www.mathworks.com/help/matlab/ref/imresize.html.

[32] "SIPI image database—misc," 2020, http://sipi.usc.edu/database/database.php?volume=misc.

[33] M. Ahmad, C. Gupta, and A. Varshney, "Digital image encryption based on chaotic map for secure transmission," in *Proceedings of the 2009 International Multimedia, Signal Processing and Communication Technologies*, pp. 292–295, IEEE, Aligarh, India, March 2009.

[34] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13951–13976, 2016.

[35] M. Ahmad and O. Farooq, "Chaos based PN sequence generator for cryptographic applications," in *Proceedings of the 2011 International Conference on Multimedia, Signal Processing and Communication Technologies*, pp. 83–86, IEEE, Aligarh, India, December 2011.