sensors

MDPI

Article

Multimedia Cryptosystem for IoT Applications Based on a Novel Chaotic System Around a Predefined Manifold

Li Li [1], Ahmed A. Abd El-Latif [2,*], Sajad Jafari [3,4], Karthikeyan Rajagopal [5], Fahimeh Nazarimehr [3] and Bassem Abd-El-Atty [6]

1 Shenzhen Institute of Information Technology, Shenzhen 518172, China; lili_sziit2014@163.com
2 Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
3 Department of Biomedical Engineering, Amirkabir University of Technology, 424 Hafez Ave., Tehran 15875-4413, Iran; sajadjafari83@gmail.com (S.J.); fahimenazarimehr@yahoo.com (F.N.)
4 Health Technology Research Institute, Amirkabir University of Technology, No. 350, Hafez Ave., Valiasr Square, Tehran 159163-4311, Iran
5 Center for Nonlinear Systems, Chennai Institute of Technology, Chennai 600069, India; karthikeyan.rajagopal@citchennai.net
6 Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt; bassem.abdelatty@fci.luxor.edu.eg
* Correspondence: aabdellatif@nu.edu.eg

Abstract: Multimedia data play an important role in our daily lives. The evolution of internet technologies means that multimedia data can easily participate amongst various users for specific purposes, in which multimedia data confidentiality and integrity have serious security issues. Chaos models play an important role in designing robust multimedia data cryptosystems. In this paper, a novel chaotic oscillator is presented. The oscillator has a particular property in which the chaotic dynamics are around pre-located manifolds. Various dynamics of the oscillator are studied. After analyzing the complex dynamics of the oscillator, it is applied to designing a new image cryptosystem, in which the results of the presented cryptosystem are tested from various viewpoints such as randomness, time encryption, correlation, plain image sensitivity, key-space, key sensitivity, histogram, entropy, resistance to classical types of attacks, and data loss analyses. The goal of the paper is proposing an applicable encryption method based on a novel chaotic oscillator with an attractor around a pre-located manifold. All the investigations confirm the reliability of using the presented cryptosystem for various IoT applications from image capture to use it.

Keywords: multimedia cryptosystem; IoT applications; chaotic systems; image security

Citation: Li, L.; Abd El-Latif, A.A.; Jafari, S.; Rajagopal, K.; Nazarimehr, F.; Abd-El-Atty, B. Multimedia Cryptosystem for IoT Applications Based on a Novel Chaotic System Around a Predefined Manifold. *Sensors* **2022**, *22*, 334. https://doi.org/10.3390/s22010334

Academic Editors: Mohammed Amin Almaiah, Omar Almomani, Yassine Maleh and Ahmad Al-Khasawneh

Received: 23 November 2021
Accepted: 28 December 2021
Published: 3 January 2022

1. Introduction

Developments in the Internet of Things (IoT), cloud computing, and fifth-generation network technologies make multimedia data easy to share with various users for specific purposes. In this context, the sharing of multimedia data suffers from serious security issues [1–4]. Multimedia data can be secured via executing one of the protection techniques: information hiding and data encryption mechanisms. Encryption techniques aim to transform multimedia data from an understood pattern to an incomprehensible form. Recently, chaos systems have played an important role in designing robust multimedia data encryption mechanisms and secure communication.

Chaotic oscillations are very complex dynamics, and there are many ambiguities about them. Many studies try to clarify the creation of chaotic dynamics [5]. Formerly, there was an idea that chaotic dynamics are related to saddle equilibria [6]. Then, some chaotic systems were proposed that do not have a saddle point [7]. Recently, many studies have been done on the investigation of chaotic oscillators with different properties [8]. Some examples of chaotic systems with various types of equilibria are given [5]. A chaotic

oscillator with a line of equilibria was studied in [9]. In [10], hyperchaotic dynamics in a system without equilibria were discussed. The application of a chaotic oscillator with no equilibria was studied in [11]. Multistability is an exciting property of a dynamic system. The multistability of a new version of the Chua system was discussed in [12]. Furthermore, multistability as a feature of a hyperjerk was studied in [13]. Extreme multistability is a feature in which the system has a complete bifurcation diagram by changing initial conditions, not parameters [14]. Memristive neural models were studied in [15]. Chaotic flows have various engineering applications such as chaotic circuit [16].

Proposing chaotic systems with dynamics around a predefined manifold has been an exciting topic. In this paper, a novel chaotic oscillator is presented. The oscillator has a particular property in which the chaotic dynamics are around pre-located manifolds. Various dynamics of the oscillator are studied. The chaotic attractor and the predefined manifolds are discussed, and their relation with equilibrium points is investigated. Studying the bifurcation diagrams of the proposed system by different initiation methods shows the multistability of the system in some intervals of the bifurcation parameter. Lyapunov exponents of the oscillator are studied to show the interval of chaotic dynamics. In the multistability region, the exciting basin of attraction of various attractors is studied.

Digital images are widely used for representing multimedia data in numerous applications. The complexity of chaotic time series makes them a proper choice for image encryption and secure communication [17–19]. Nonlinear methods are useful in image encryption [20–22]. The application of a chaotic oscillator in fingerprint encryption was discussed in [23]. In [24], image encryption using a chaotic map was studied. Moreover, the encryption of medical images using a chaotic map was discussed in [25], and applying an exponential chaotic oscillator in secure communication was investigated in [26].

Based on the nonlinear features of the presented chaotic oscillator system, we present a novel image cryptosystem for IoT applications, in which the results of the presented cryptosystem are tested from various viewpoints. All the investigations show the reliability of the image cryptosystem for various IoT applications.

The presented contributions of this work can be outlined as follows:

- Presenting a novel chaotic oscillator, in which the chaotic dynamics are around pre-located manifolds.
- Designing a novel image cryptosystem for IoT applications, of which the design is based on the nonlinear features of the presented chaotic oscillator system.

2. Proposed Framework for IoT Environment

Multimedia data, such as images, audio, and video are growing rapidly as an essential avenue for the representing, sharing, and storage of data in our daily lives. The evolution of internet technologies makes multimedia data can easily stored in cloud storage and shared amongst various users for specific goals. In this context, the confidentiality and integrity of multimedia data suffer from serious security issues. Therefore, we proposed a new framework for IoT applications to store and share digital images, in which image data confidentiality and integrity are achieved. The proposed framework is presented in Figure 1.

The presented image cryptosystem can be utilized in different application fields, such as the medical sector, surveillance systems, personal data protection, etc. In the medical sector, the presented image cryptosystem can be utilized for the secure transmission of medical images from their origin to the intended stakeholders for analyzing, assessing, and treat patients. In surveillance systems, when the system detects any movement in the camera location, the video frames are captured and encrypted via the presented cryptosystem then sent the encrypted data to the intended stakeholders for analyzing and taking the appropriate decision. Moreover, the presented cryptosystem can be utilized for storing multimedia data to cloud storage then sharing/downloading it up to require.

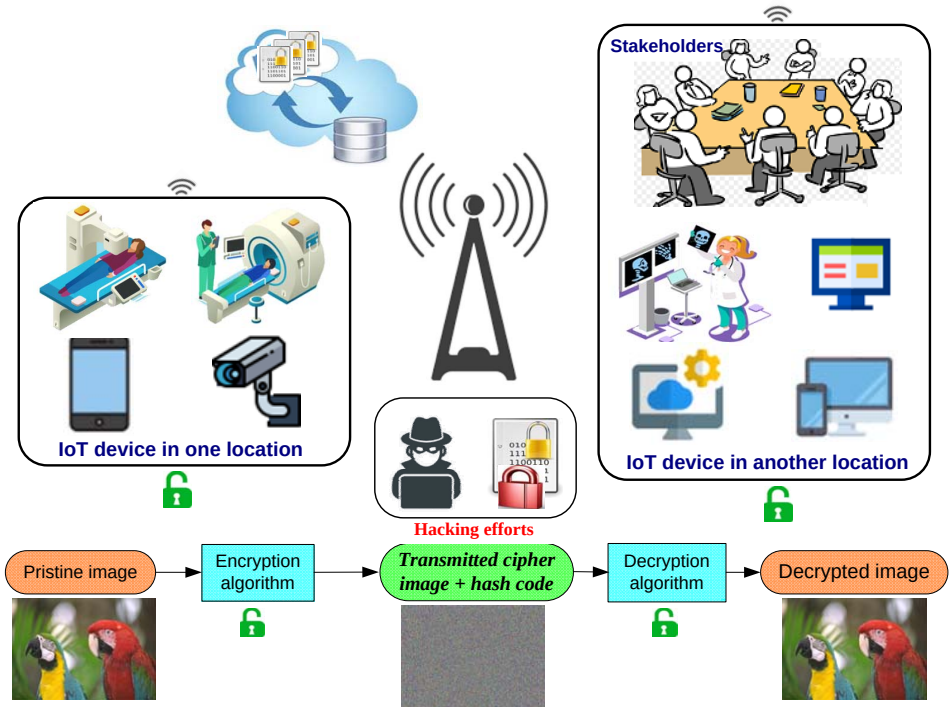


Figure 1. Proposed framework for the secure transmission of multimedia data in IoT environment.

To maintain the integrity of the transmitted data via our presented cryptosystem, we utilized a hashing algorithm like SHA-256. The hashing algorithm is employed to get the hash code for the appended secret key with the cipher multimedia (secret key + cipher data), for making SHA-256 a keyed hash algorithm, then the generated hash code is sent with the cipher data. Upon the intended user downloaded the encrypted data and receiving the hash code, the hash value is computed for the received cipher data with the secret key, and investigate if the generated hash value is the same as the received hash code or not. If the two hash values are the same, then there are no changes in the transmitted cipher data, and the integrity of transmitted data has been achieved.

3. Proposed Chaotic Oscillator System

In this paper, a chaotic oscillator with a unique feature is proposed as Equation (1).

$$\begin{aligned} \dot{x} &= z \\ \dot{y} &= x^2 + y^2 - 1 \\ \dot{z} &= -2x - y + az + xy \end{aligned} \tag{1}$$

The system presents a chaotic dynamic in $a = 0$, and initial values $(x_0, y_0, z_0) = (0, 0, 0)$. Its Lyapunov exponents are $(0.1322, 0, -0.9518)$. Three projections and the 3D chaotic solution of the oscillator are shown in Figure 2. Figure 3 presents signals of various variables for the chaotic dynamic. In order to have bounded solutions, the derivative of variables should be zeros. So, the system's dynamics should be around the pre-located manifolds as $z = 0, x^2 + y^2 = 1$, and $y = \frac{2x}{x-1}$. The chaotic dynamic and these manifolds are plotted in Figure 4.

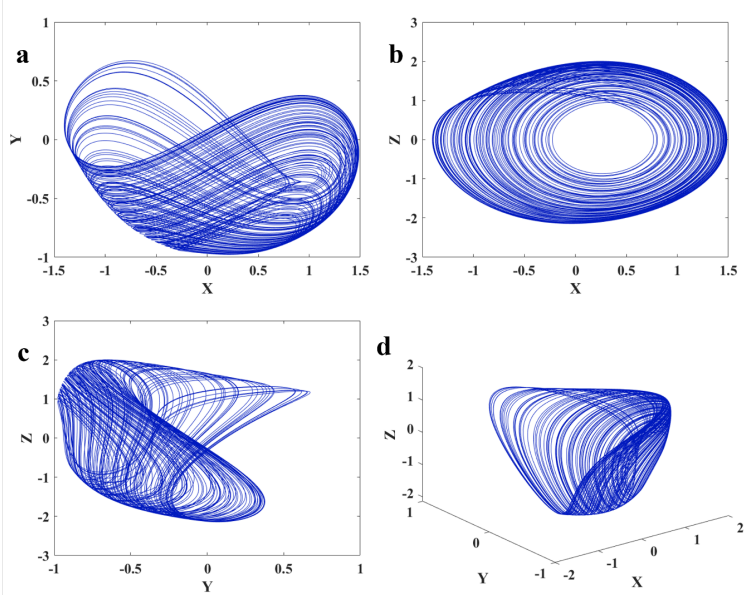


Figure 2. The chaotic dynamics of Equation (1) with $a = 0$ and $(x_0, y_0, z_0) = (0, 0, 0)$ in (**a**) $X - Y$; (**b**) $X - Z$; (**c**) $Y - Z$; (**d**) $X - Y - Z$.

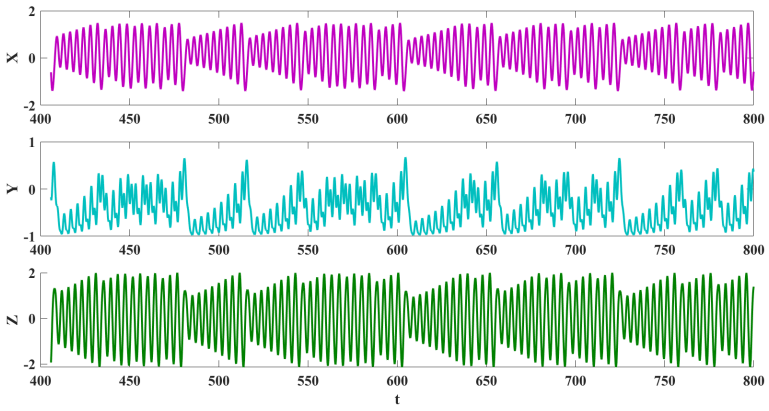


Figure 3. Time series of Equation (1) with $a = 0$ and $(x_0, y_0, z_0) = (0, 0, 0)$.

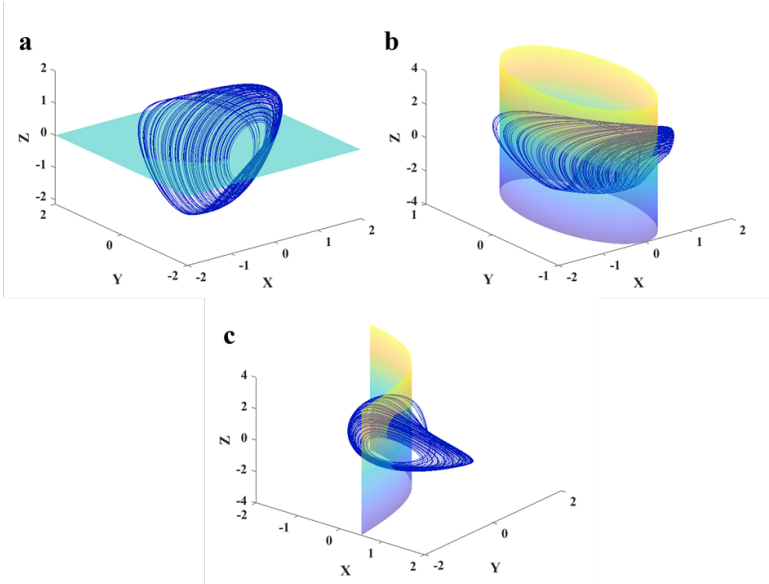


Figure 4. 3D chaotic dynamics of Equation (1) and the three pre-located manifolds (**a**–**c**).

4. Dynamical Properties of the Oscillator

4.1. Equilibrium Points

To calculate the equilibrium points of the oscillator, all of its derivatives should be zeros simultaneously. So we can tell that the intersections of the three studied manifolds are the equilibria of the system. Equation (1) has two equilibrium points as $E_1 = (0.3213, -0.947, 0), E_2 = (-0.6323, 0.7747, 0)$. In parameter $a = 0$, the eigenvalues of the oscillator for E_1 are $(-1.9582, 0.0322 \pm 1.7528i)$, and for Eq_2 are $(1.9576, -0.2041 \pm 1.4081i)$. So, the equilibrium points are saddle points. It means that the chaotic dynamics are self-excited.

4.2. Bifurcation Diagram and Lyapunov Exponents

To study different dynamics of the oscillator, the bifurcation diagram is presented in Figure 5. In these diagrams, the maximum values of the three variables are plotted by changing bifurcation parameter a. The diagram is plotted by the backward continuation method, and the first set of initial conditions are $(0, 0, 0)$. A period-doubling route to chaos can be seen in the bifurcation diagram. To confirm the existence of chaos, Lyapunov exponents (LEs) are computed with run time 20,000. Figure 6 presents the diagram of LEs by changing parameter a, corresponding to the bifurcation diagram. One positive LE shows chaotic behaviors.

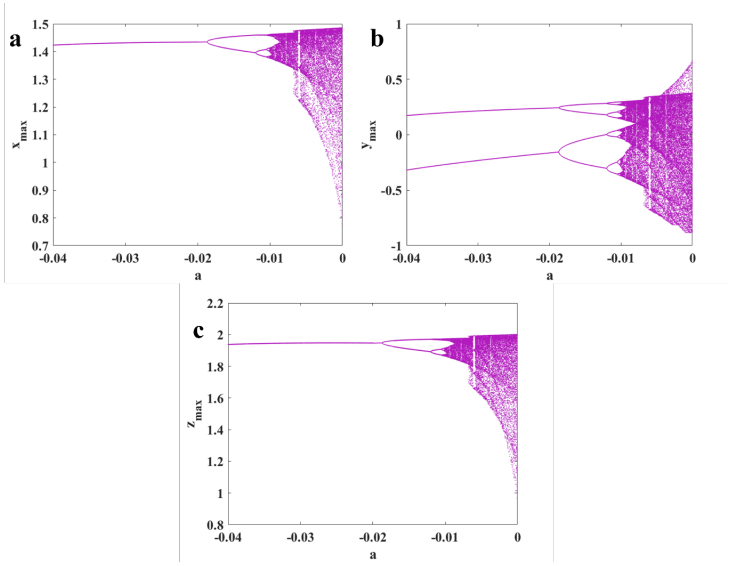


Figure 5. Bifurcation diagram of Equation (1) by changing parameter a and backward continuation method; maximum values of (**a**) x variable; (**b**) y variable; (**c**) z variable.

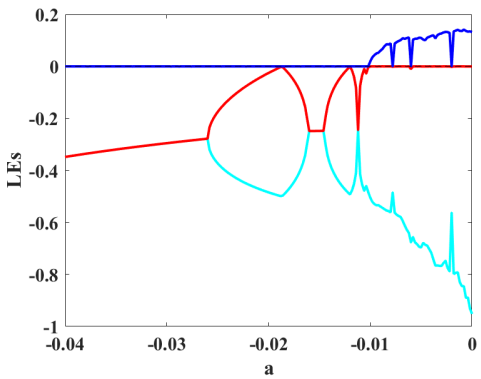


Figure 6. The diagram of LEs by changing parameter a.

4.3. Multistability Analysis

Multistability is one of the exciting features of dynamical systems. It means that two different sets of initial conditions result in two different attractors. The multistability of the oscillator is examined by plotting bifurcation diagrams using two different initiation methods, backward and constant initiation. Figure 7 shows the backward bifurcation in purple and bifurcation with constant initial conditions in blue. The results reveal the coexisting attractors in the interval $a \in [-0.0105, -0.00975]$, since the two diagrams with different initiation methods are not the same.

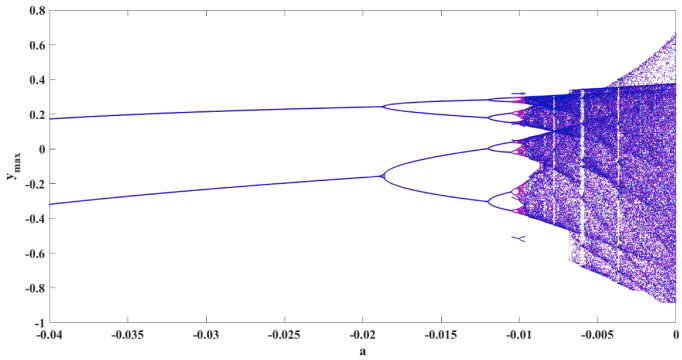


Figure 7. Bifurcation diagram of the oscillator by changing parameter a; bifurcation with backward continuation method is shown in purple and with constant initial conditions is shown in blue.

4.4. Basin of Attraction

After revealing the coexisting attractors, investigating the basin of attraction of each attractor is interesting. Figure 8 shows the basin of attraction of the oscillator in parameter $a = -0.0099$. It can be seen in Figure 7 that two periodic and chaotic dynamics coexist in this parameter. In Figure 8, the green, dark blue, and cyan regions show the basin of attraction for unbounded, periodic, and chaotic solutions.The basin of attractions of different attractors are entangled with each other.

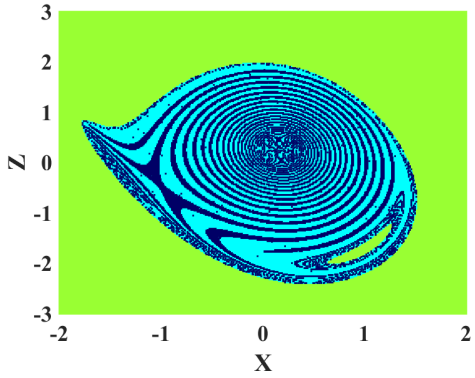


Figure 8. Basin of attraction of the oscillator; green, dark blue, and cyan regions show the basin of attraction for unbounded, periodic, and chaotic solutions, respectively.

5. The Proposed Image Encryption Approach

The protection of data represented by images can be achieved via image data protection techniques like image encryption, image data hiding, or mixing between them [27,28]. Spring from the presented chaotic system's benefits, we propose a new image encryption approach, which necessitates an adaptation for our chaotic map as presented in Equation (2).

$$\begin{cases} x_{i+1} = z_i mod 1 \\ y_{i+1} = \left(x_i^2 + y_i^2 - 1\right) mod 1 \\ z_{i+1} = (-2x_i - y_i + az_i + x_i y_i) mod 1 \end{cases} \quad (2)$$

The presented image cryptosystem employs the benefits of our chaotic system to generate three pseudo-random sequences. The first two sequences are used to permute the plain image. Then the last sequence is utilized to substitute the permuted image for constructing the cipher image. The multimedia image cryptosystem is described in Figure 9, and the encryption procedure is listed in the following steps.

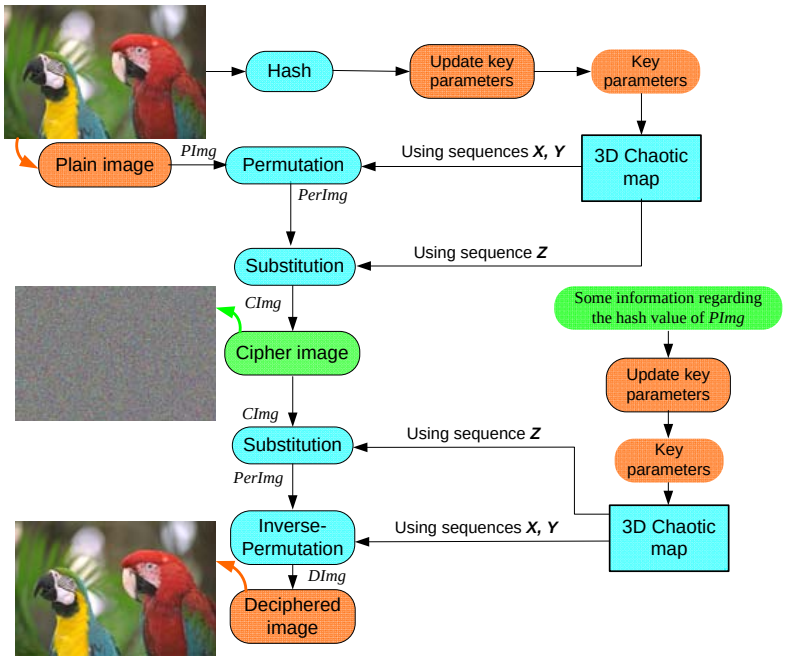


Figure 9. Description of the proposed cryptosystem for multimedia images.

1. Perform the hash function SHA256 on the plain image (*PImg*) to get the hash value (V).
2. Convert V into 32 integer numbers (v_1, v_2, v_3, ..., v_{32}) each of 8-bit, then obtain 3 decimal numbers from these integers as follows.

$$D_1 = \frac{v_1 \oplus v_2 \oplus \cdots \oplus v_{11}}{256}$$
$$D_2 = \frac{v_{12} \oplus v_{10} \oplus \cdots \oplus v_{22}}{256}$$
$$D_3 = \frac{v_{23} \oplus v_{18} \oplus \cdots \oplus v_{32}}{256}$$

3. Choose initial values for key parameters ($x_{initial}$, $y_{initial}$, $z_{initial}$) and update these keys using D_1, D_2, and D_3.

$$x_0 = \frac{x_{\text{initial}} + D_1}{2}$$
$$y_0 = \frac{y_{\text{initial}} + D_2}{2}$$
$$z_0 = \frac{z_{\text{initial}} + D_3}{2}$$

4. Iterate the chaotic system (2) for $H \times W \times L$ times using the updated key parameters (x_0, y_0, z_0, a) for generating 3 sequences (X, Y, Z), in which $H \times W \times L$ is the size of *PImg*.
5. Add the values of X to the values of Y as sequence W, then sort the values of W from the smallest to the largest as sequence S, and obtain the index S in W as *PrVc*.
6. Reshape the plain image (*PImg*) into a vector (*PImgVc*) and permute *PImgVc* using the produced vector *PrVc* as follows.

$$PerImgVc(i) = PImgVc(PrVc(i))$$

$$for \;\; i = 1, 2, ..., H \times W \times L$$

7. Construct the key sequence (K) by adapting the sequence Z into integers.

$$K = fix(Z \times 10^{12}) \mod 256$$

8. Perform Bitwise-Xor operation on the permuted vector $PerImgVc$ and K to construct the cipher image $CImg$.

$$CImgVc = PerImgVc \oplus K$$

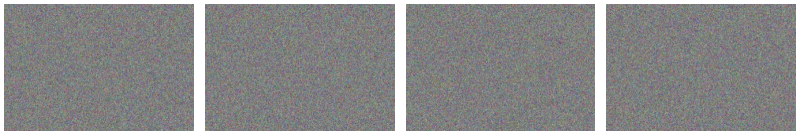
$$CImg = reshape(CImgVc, H, W, L)$$

6. Experimental Outcomes

The utilized dataset of images is obtained from the Kodak database [29]. It consists of four images named Macaws, Chalet, Window, and Houses, with size 768 × 512 (see Figure 10). The utilized initial values to iterate the 3D chaotic map are $x_{initial}$ = 0.6275, $y_{initial}$ = 0.3854, $z_{initial}$ = 0.7261, $a = 0$.

The effectiveness of any image cryptosystem depends essentially on performance (how fast we can encrypt an image on a defined computer) and resistance to various attacks: such as brute force, linear and differential cryptanalysis, statistical cryptanalysis, etc.). These two essential properties are discussed in the following subsections to show the effectiveness of the presented image cryptosystem.

(**a**) PrImg01 (**b**) PrImg02 (**c**) PrImg03 (**d**) PrImg04



(**e**) CrImg01 (**f**) CrImg02 (**g**) CrImg03 (**h**) CrImg04

Figure 10. Experimented image dataset of dimensional 768 × 512, in which the first row denotes the plain images, while the second row describes the corresponding ciphered images.

6.1. Time Efficiency

To demonstrate the effectiveness of the presented cryptosystem in terms of time encryption, Table 1 stated a superficial comparison of time encryption for the presented cryptosystem with other related encryption algorithms, as reported in [30–32]. From the stated information in Table 1, we can deduce that our cryptosystem is more superb than other ones in terms of time encryption.

Table 1. Comparison of time encryption for the presented cryptosystem with other related cryptosystems, as reported in [30–32].

Image Cryptosystem	Number of Encrypted Bits Per Second
Proposed	9,713,394
Ref. [30]	8,025,072
Ref. [31]	6,381,110
Ref. [32]	4,224,509

6.2. Randomness Analysis

For testing the randomness of the created sequence constructed the cipher image, we perform NIST SP 800-22 tests composed of fifteen tests. These tests are applied on a

2,000,000-bit of the constructed Cipher–Macaws image and its utilized key-stream. The outcomes are provided in Table 2, which declares that all NIST SP 800-22 tests are passed successfully. Consequently, the presented 3D chaotic system can be reliable in designing various modern cryptographic applications.

Table 2. Outcomes of randomness test.

Test-Name	*p*-Value		Passed
	Key Stream	Cipher-Macaws	
Runs	0.7913189	0.5294244	✓
DFT	0.6543473	0.6036850	✓
Linear complexity	0.7024604	0.1581112	✓
Block-frequency	0.5686530	0.3487918	✓
Frequency	0.6559749	0.4300353	✓
Universal	0.3457104	0.9949709	✓
Serial test 1	0.3920807	0.3989737	✓
Serial test 2	0.5967691	0.5770354	✓
Overlapping templates	0.7827032	0.4365690	✓
No overlapping templates	0.9636127	0.5941496	✓
Long runs of ones	0.3969673	0.7129090	✓
Approximate entropy	0.2772607	0.1420810	✓
Rank	0.0996206	0.5740640	✓
Random excursions variant x = 1	0.0963609	0.6213966	✓
Random excursions x = 1	0.3570832	0.8722024	✓
Cumulative sums (reverse)	0.0620619	0.5399098	✓
Cumulative sums (forward)	0.1740884	0.7368549	✓

6.3. Correlation Analysis

To study the perception of an image, we employ the correlation coefficient (*CC*) of adjacent pixels. Ordinary images possess *CC* near 1 in each direction. Cipher images (constructed using a robust-designed image cryptosystem) should be approximately 0. To calculate *CC* for the original and encrypted images, we picked 10,000 pairs of adjacent pixels at random in every direction.

$$CC = \frac{\sum_{x=1}^{A}(p_x - \bar{p})(c_x - \bar{c})}{\sqrt{\sum_{x=1}^{A}(p_x - \bar{p})^2 \sum_{x=1}^{N}(c_x - \bar{c})^2}} \tag{3}$$

where A indicates the entire number of adjacent pixel pairs and c_x, p_x indicate the adjacent pixels. Table 3 presents the outcomes of CC for encrypted images and plain ones, in which the *CC* for cipher images is approximately 0. Additionally, Figures 11–13 plot the distribution of correlation per direction in Macaws image and its encrypted one. From the outcomes provided in Table 3 and shown in Figures 11–13, no valuable information was gained regarding the plain image by analyzing CC values.

Table 3. Correlation coefficient of neighboring pixels for the experimented images.

Image	Direction								
	Hor.			Ver.			Dia.		
	R	G	B	R	G	B	R	G	B
Macaws	0.98685	0.98074	0.98562	0.98874	0.98460	0.98550	0.98024	0.97349	0.97804
Cipher-Macaws	−0.00001	−0.00005	0.00073	0.00026	0.00051	−0.00078	−0.00010	0.00056	−0.00125
Chalet	0.93698	0.92077	0.91862	0.94179	0.93844	0.92290	0.91195	0.90044	0.89372
Cipher-Chalet	0.00083	−0.00002	0.00006	0.00044	−0.00044	0.00114	−0.00017	−0.00018	0.00058
Window	0.95772	0.94235	0.95532	0.97114	0.96285	0.96658	0.93616	0.92107	0.93504
Cipher-Window	0.00087	−0.00088	−0.00066	0.00012	0.00062	0.00144	0.00007	0.00033	−0.00008
Houses	0.92373	0.92224	0.90793	0.88870	0.88994	0.86135	0.82085	0.81976	0.77976
Cipher-Houses	0.00085	−0.00004	−0.00066	0.00059	0.00072	0.00061	−0.00040	0.00128	−0.00075

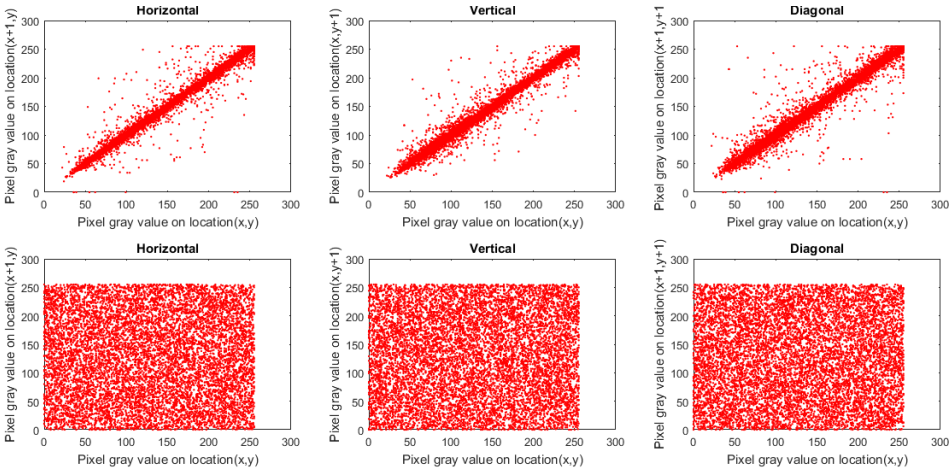


Figure 11. Plots of correlation distribution (in each direction) for Macaws image (Red channel), in which the first row denotes the plain Macaws image, while the bottom row signifies the ciphered Macaws image.

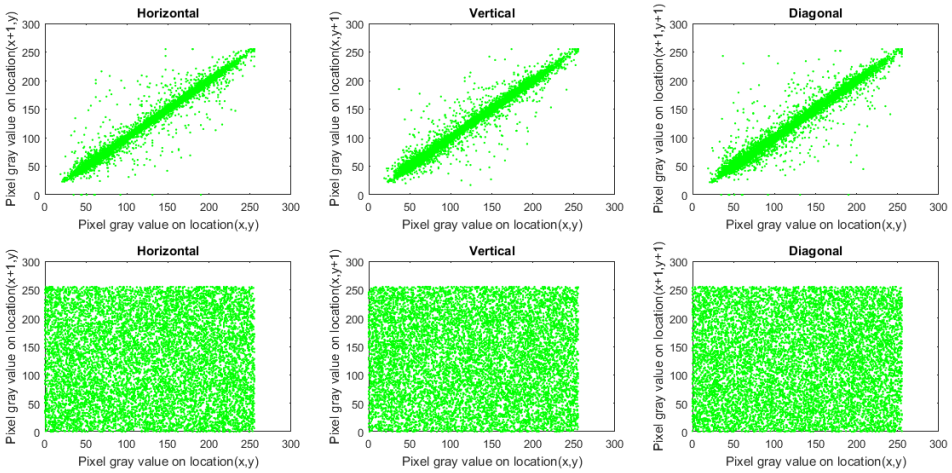


Figure 12. Plots of correlation distribution (in each direction) for Macaws image (Green channel), in which the first row denotes the plain Macaws image, while the bottom row signifies the ciphered Macaws image.

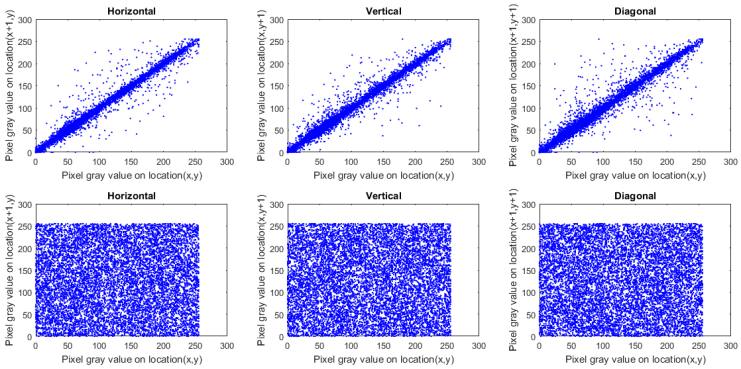


Figure 13. Plots of correlation distribution (in each direction) for Macaws image (Blue channel), in which the first row denotes the plain Macaws image, while the bottom row signifies the ciphered Macaws image.

6.4. Differential Analysis

Plain-image sensitivity refers to any tiny modifications on the plain image, resulting in a massive difference for the cipher image. To test plain-image sensitivity for our image cryptosystem, we employ NPCR ("Number of Pixel Change Rate") and UNCI ("Unified Average Changing Intensity"), which are represented as follows,

$$\begin{aligned} NPCR &= \frac{\sum_{i,j} Df(i,j)}{A} \times 100\%, \\ Df(i,j) &= \begin{cases} 0 \; if \; C1(i,j) = C2(i,j) \\ 1 \; if \; C1(i,j) \neq C2(i,j) \end{cases} \end{aligned} \tag{4}$$

$$UACI = \frac{1}{A}\left(\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255}\right) \times 100\% \tag{5}$$

where A denotes the full number of image pixels and $C1$, $C2$ denote the two ciphered images for a plain image differs in one bit. The outcomes of NPCR and UNCI are stated in Table 4. It demonstrates our image cryptosystem enjoys high sensitivity to slight modifications in the original image.

Table 4. Outcomes of NPCR and UNCI.

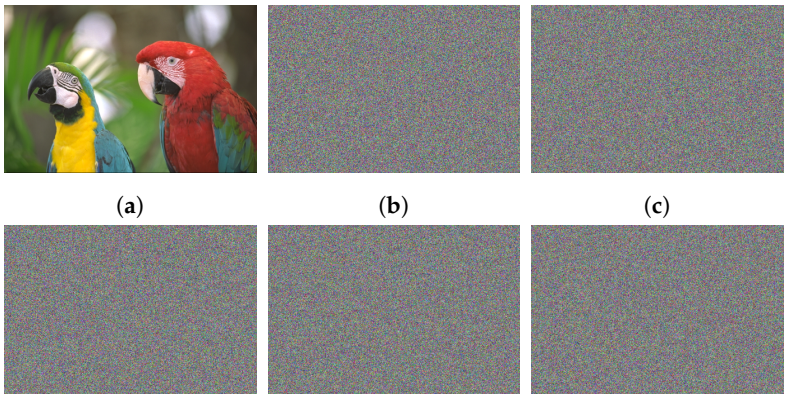
Image	NPCR	UNCI
Macaws	99.60556%	33.49106%
Chalet	99.61565%	33.45562%
Window	99.60988%	33.47213%
Houses	99.60751%	33.44994%

6.5. Key-Space Analysis

Multifarious secret keys that can be utilized in brute force attacks are known as key-space. By the benchmark stated in [33], the key-space ought to be larger than 2^{100} to demonstrate sufficient security against brute-force attacks. The presented image cryptosystem uses initial key parameters ($x_{initial}$, $y_{initial}$, $z_{initial}$, and a) to generate the chaotic sequences utilized in encryption and decryption procedures. By assuming the precision of computation for digital devices is 10^{-16}, then the key-space for the presented mechanism is $\simeq 2^{213}$, which is immense sufficiently for any cryptographic algorithm.

6.6. Key Sensitivity Analysis

It is defined as the sensitivity of the decryption to the secret key. It is a necessary measure to guarantee the reliability of any cryptosystem. For evaluating the suggested image cryptosystem's key sensitivity, the Cipher-Macaws image is deciphered many times using slight changes in the secret key as displayed in Figure 14.



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 14. Outcomes of decrypting Cipher–Macaws image using slight changes in the confidential key. (**a**) The confidential key; (**b**) The confidential key except $x_{initial}$ = 0.627500000000001; (**c**) The confidential key except $y_{initial}$ = 0.3854000000000001; (**d**) The confidential key except $z_{initial}$ = 0.7261000000000001; (**e**) The confidential key except $x_{initial}$ = 0.627499999999999; (**f**) The confidential key except $y_{initial}$ = 0.38539999999999.

6.7. Histogram Analysis

To evaluate the pixel values' distribution in the encrypted images, the histogram test is employed. A proper image cryptosystem has to guarantee the identical distribution for varied cipher images. Figure 15 plots the histograms of the studied images. The histograms of the plain images are not similar, while the histograms of their related ciphered ones are uniform. Additionally, we applied chi-square (χ^2) analysis to guarantee the histogram results.

$$\chi^2 = \sum_{j=0}^{255} \frac{(f_j - D)^2}{D} \tag{6}$$

where D denotes the image dimension and f_j represents the frequency of the pixel value j. By considering the significant level β=0.05, then $\chi^2_\beta(255) = 293.3$ is obtained. For an image, when the χ^2 value is less than $\chi^2_\beta(255)$, then the histogram of this image is uniform. Table 5 provides the outcomes of χ^2 for the studied images, in which the χ^2 outcomes for all encrypted images are less than $\chi^2_\beta(255)$. So, the proposed image cryptosystem can withstand attacks of histogram analysis.

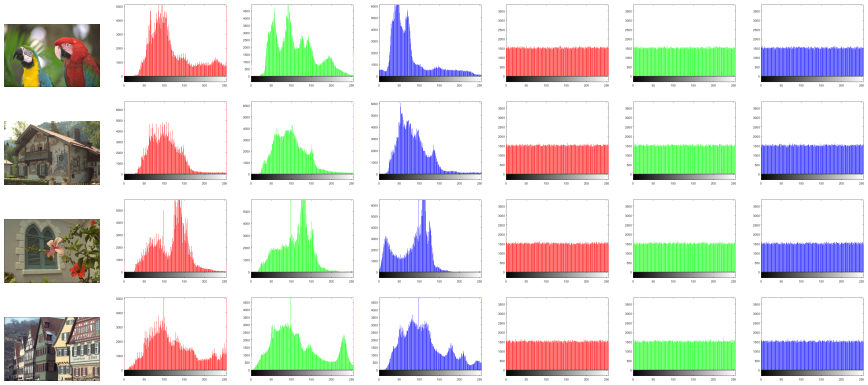


Figure 15. Plots of histograms for experimented images, in which the left three columns except the first one represent the histograms of plain images, while the right three columns represent the histograms of cipher images.

Table 5. χ^2 outcomes for the investigated images.

Image	χ^2 Value			Outcome
	Red	Green	Blue	
Macaws	303,687.9661	254,324.4518	603,349.4934	Irregular
Chalet	817,766.5013	677,362.4271	616,936.1705	Irregular
Window	515,942.4335	551,843.4661	728,008.0781	Irregular
Houses	285,277.4635	219,680.6289	221,228.6081	Irregular
Cipher-Macaws	244.5221	251.6953	233.6315	Regular
Cipher-Chalet	258.3451	215.8021	243.8919	Regular
Cipher-Window	209.8372	277.1874	254.2682	Regular
Cipher-Houses	226.9335	248.9882	241.1497	Regular

6.8. Entropy Analysis

To evaluate the bit distribution for each level of the pixel values of the encrypted image, the global entropy is employed as follows:

$$E(X) = -\sum_{j=0}^{255} r(x_j) \log_2(r(x_j)) \tag{7}$$

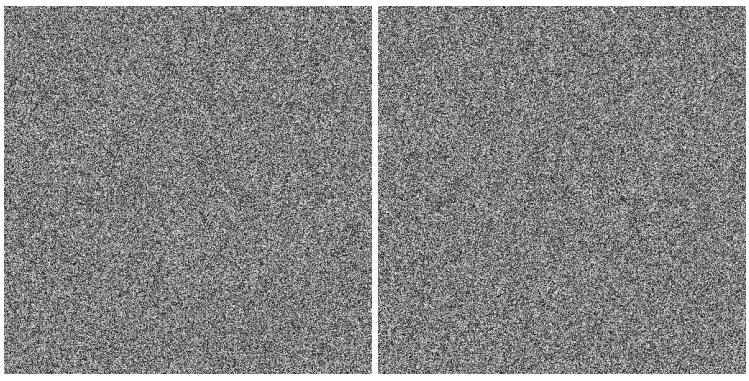
where $r(x_j)$ is the probability of x_j. The possible values of a grayscale image are 2^8, so the optimal entropy is 8-bit. Subsequently, to assess the efficacy of the suggested cryptosystem, the entropy of the ciphered images should be near to 8. The global entropy neglects the assessment of real randomness for cipher images. Therefore, we employ local entropy to assess the actual randomness for cipher images which can be computed via the average global entropies for no overlapping blocks (the size of each block is 44×44). Table 6 shows the results of local and global entropies for the experimented images, in which all outcomes of information entropy for cipher images are approximately 8-bit. Consequently, the proposed cryptosystem is robust against entropy attacks.

Table 6. Local and global information entropies.

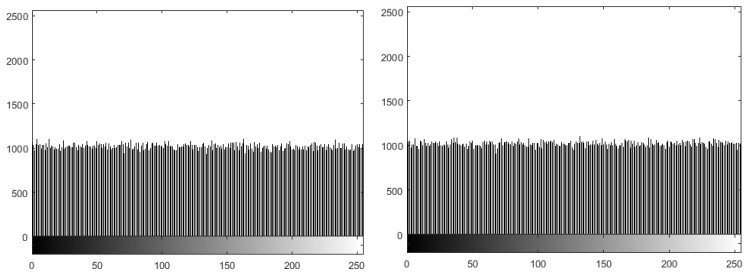
Image	Global Entropy		Local Entropy	
	Plain	**Cipher**	**Plain**	**Cipher**
Macaws	7.601941	7.999837	5.396978	7.902671
Chalet	7.136653	7.999834	5.673345	7.903744
Window	7.309858	7.999855	5.441143	7.902341
Houses	7.673795	7.999874	6.552062	7.902232

6.9. Classical Types of Attack

In general, the cryptanalysis of a cryptosystem assumes that cryptanalysts fully understand the structure of the cryptosystem and know all things about the encryption and decryption algorithms except the secret key utilized in encryption and decryption procedures. There are four kinds of attacks: ciphertext-only, chosen-ciphertext, chosen-plaintext, and known-plaintext [30]. The chosen-plaintext attack is considered to be the most effective attack in which the cyberpunk has temporary access to the cryptosystem and can create the ciphertext associated with the selected plaintext. If an encryption algorithm is able to resist the chosen-plaintext attack, it has the capability to resist other kinds of attacks. In the proposed encryption algorithm, if any of the initial keys ($x_{initial}$, $y_{initial}$, $z_{initial}$, and a) have a slight modification, the outcome will change vastly. Furthermore, our encryption approach applies SHA256 to the plain image for updating the initial parameters, so that our cryptosystem not only depends on the secret key but also on the plain image. The cryptanalyst attempts to acquire useful information about the secret key utilizing all-white and all-black images, as they can disable the task of permutation/substitution procedures. The affiliated cipher images for the all-white and all-black images and their related histograms are provided in Figure 16, in which no visual information can be acquired from these cipher images, while Table 7 supplies some statistical analyses for these images. As a result, our cryptosystem has the capability to resist linear cryptanalysis.



(**a**) Cipher all-black (**b**) Cipher all-white



(**c**) Histogram of cipher all-black (**d**) Histogram of cipher all-white

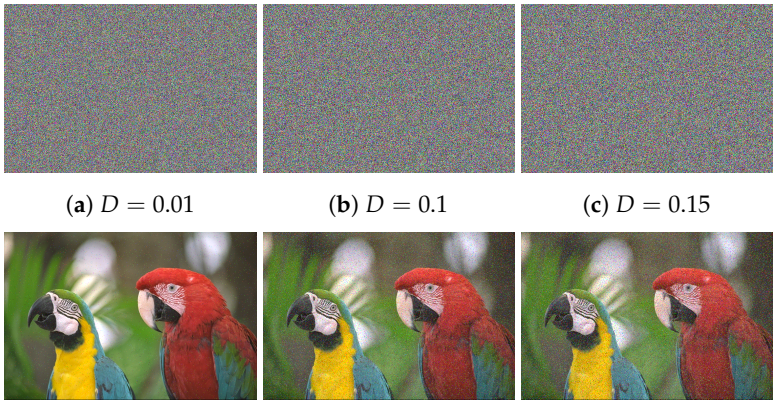
Figure 16. Ciphers of all-black and all-white images, and their analog histograms.

Table 7. Statistical analyses of the cipher all-black and all-white images.

Image	Correlation			χ^2 Value	Entropy	
	Hor.	Ver.	Dia.		Global	Local
All-black	−0.0002	−0.0004	0.0001	267.7656	7.99926	7.90340
All-white	0.0006	0.0001	0.0004	226.8008	7.99937	7.90343

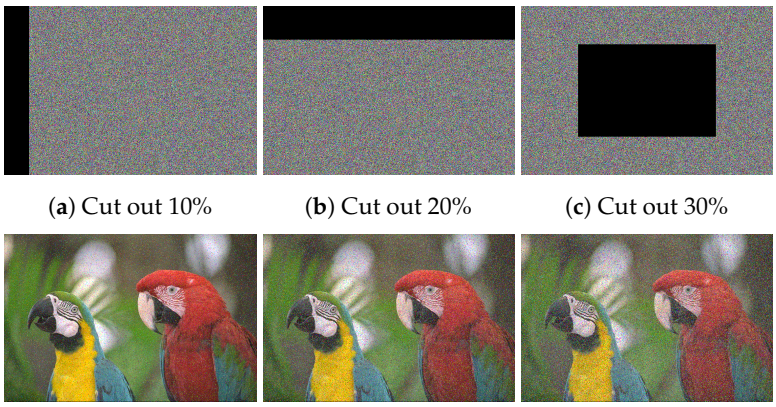
6.10. Occlusion Analysis

It is significant that most of the data transmission networks are noisy channels. Once data are transmitted over noisy networks, it is probably distorted by noise or data loss attacks. So, a well-designed cryptosystem should withstand data loss and noise attacks. For investigating the proposed image cryptosystem for facing data loss and noise attacks, we defect the Cipher–Macaws image via performing a cutting block for data with various sizes or applying Salt and Pepper noise with variable densities. Then we decipher the defective image. The outcomes of noise and data loss attacks are displayed in Figures 17 and 18, respectively. The deciphered images have a well-visual quality with no lack of visual details inside the area of the cutting portion.



(**a**) $D = 0.01$ (**b**) $D = 0.1$ (**c**) $D = 0.15$

Figure 17. Outcomes of noise attack, in which the top row refers to the defective Cipher–Macaws image by adding Salt and Pepper noise with variable densities (D) while the bottom row represents the corresponding decipher image.



(**a**) Cut out 10% (**b**) Cut out 20% (**c**) Cut out 30%

Figure 18. Outcomes of data loss attack, in which the top row refers to the defective Cipher–Macaws image by performing a cutting block for data with various sizes, while the bottom row represents the corresponding decipher image.

7. Conclusions

A novel chaotic flow was proposed in this paper in which its attractor was around some predefined manifolds. The bifurcation diagram of the system has exhibited a period-doubling route to chaos by modifying parameter a. Lyapunov exponents of the system were presented to determine the chaotic interval of the parameter. The multistability of the system was revealed by plotting bifurcation diagrams using different initiation methods. The basin of attraction of the attractors was studied. The proposed system was used in a multimedia image cryptosystem. The results were examined using different analyses such as randomness, correlation, plain image sensitivity, key sensitivity, histogram, entropy, and data damage analyses. The results of these tests confirm the reliability of using the presented cryptosystem for various IoT applications from image capture to use it.

Author Contributions: Conceptualization, A.A.A.E.-L.; methodology, F.N., B.A.-E.-A.; software, F.N., B.A.-E.-A.; formal analysis, A.A.A.E.-L., S.J., B.A.-E.-A.; investigation, A.A.A.E.-L.; resources, L.L., F.N.; data curation, S.J.; writing—original draft preparation, A.A.A.E.-L., B.A.-E.-A.; writing—review and editing, S.J., K.R.; supervision, K.R.; project administration, L.L.; funding acquisition, L.L. All authors have read and agreed to the published version of the manuscript.

Funding: The paper is supported by Shenzhen Institute of Information Technology, funding number: SZIIT2021KJ040

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Acknowledgments: Bassem Abd-El-Atty acknowledges support from Luxor University, Egypt. Ahmed A. Abd EL-Latif acknowledges support from Menoufia University, Egypt.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. El-Latif, A.A.A.; Abd-El-Atty, B.; Mazurczyk, W.; Fung, C.; Venegas-Andraca, S.E. Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 118–131. [CrossRef]
2. Bubukayr, M.A.S.; Almaiah, M.A. Cybersecurity concerns in smart-phones and applications: A survey. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 725–731.
3. Almaiah, M.A. A New Scheme for Detecting Malicious Attacks in Wireless Sensor Networks Based on Blockchain Technology. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer: Cham, Switzerland, 2021; pp. 217–234.
4. AlMedires, M.; AlMaiah, M. Cybersecurity in Industrial Control System (ICS). In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 640–647.
5. Zhang, S.; Wang, X.; Zeng, Z. A simple no-equilibrium chaotic system with only one signum function for generating multidirectional variable hidden attractors and its hardware implementation. *Chaos Interdiscip. J. Nonlinear Sci.* **2020**, *30*, 053129. [CrossRef] [PubMed]
6. Rössler, O.E. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
7. Wang, X.; Chen, G. A chaotic system with only one stable equilibrium. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 1264–1272. [CrossRef]
8. Petrzela, J. Strange Attractors Generated by Multiple-Valued Static Memory Cell with Polynomial Approximation of Resonant Tunneling Diodes. *Entropy* **2018**, *20*, 697. [CrossRef]
9. Moysis, L.; Volos, C.; Stouboulos, I.; Goudos, S.; Çiçek, S.; Pham, V.T.; Mishra, V.K. A Novel Chaotic System with a Line Equilibrium: Analysis and Its Applications to Secure Communication and Random Bit Generation. *Telecom* **2020**, *1*, 283–296. [CrossRef]
10. Escalante-González, R.J.; Campos, E. Hyperchaotic attractors through coupling of systems without equilibria. *Eur. Phys. J. Spec. Top.* **2020**, *229*, 1309–1318. [CrossRef]
11. Wang, X.; Çavuşoğlu, Ü.; Kacar, S.; Akgul, A.; Pham, V.T.; Jafari, S.; Alsaadi, F.E.; Nguyen, X.Q. S-box based image encryption application using a chaotic system without equilibrium. *Appl. Sci.* **2019**, *9*, 781. [CrossRef]
12. Wang, N.; Zhang, G.; Kuznetsov, N.V.; Bao, H. Hidden attractors and multistability in a modified Chua's circuit. *Commun. Nonlinear Sci. Numer. Simul.* **2021**, *92*, 105494. [CrossRef]

13. Leutcho, G.D.; Kengne, J.; Kengne, L.K.; Akgul, A.; Pham, V.T.; Jafari, S. A novel chaotic hyperjerk circuit with bubbles of bifurcation: mixed-mode bursting oscillations, multistability, and circuit realization. *Phys. Scr.* **2020**, *95*, 075216. [CrossRef]
14. Zhang, Y.; Liu, Z.; Wu, H.; Chen, S.; Bao, B. Extreme multistability in memristive hyper-jerk system and stability mechanism analysis using dimensionality reduction model. *Eur. Phys. J. Spec. Top.* **2019**, *228*, 1995–2009. [CrossRef]
15. Bao, H.; Liu, W.; Ma, J.; Wu, H. Memristor initial-offset boosting in memristive HR neuron model with hidden firing patterns. *Int. J. Bifurc. Chaos* **2020**, *30*, 2030029. [CrossRef]
16. Gong, L.; Wu, R.; Zhou, N. A New 4D Chaotic System with Coexisting Hidden Chaotic Attractors. *Int. J. Bifurc. Chaos* **2020**, *30*, 2050142, [CrossRef]
17. Hua, Z.; Zhu, Z.; Yi, S.; Zhang, Z.; Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci.* **2021**, *546*, 1063–1083. [CrossRef]
18. Ravichandran, D.; Murthy, B.; Balasubramanian, V.; Fathima, S.; Amirtharajan, R.; et al. An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. *Med. Biol. Eng. Comput.* **2021**, *59*, 589–605. [CrossRef] [PubMed]
19. Dai, J.Y.; Ma, Y.; Zhou, N.R. Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henon map. *Quantum Inf. Process.* **2021**, *20*, 1–24. [CrossRef]
20. Duan, C.F.; Zhou, J.; Gong, L.H.; Wu, J.Y.; Zhou, N.R. New color image encryption scheme based on multi-parameter fractional discrete Tchebyshev moments and nonlinear fractal permutation method. *Opt. Lasers Eng.* **2022**, *150*, 106881. [CrossRef]
21. Tong, L.J.; Zhou, N.R.; Huang, Z.J.; Xie, X.W.; Liang, Y.R. Nonlinear Multi-Image Encryption Scheme with the Reality-Preserving Discrete Fractional Angular Transform and DNA Sequences. *Secur. Commun. Netw.* **2021**, *2021*. [CrossRef]
22. Almaiah, M.A.; Dawahdeh, Z.; Almomani, O.; Alsaaidah, A.; Al-khasawneh, A.; Khawatreh, S. A new hybrid text encryption approach over mobile ad hoc network. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 6461–6471. [CrossRef]
23. Lai, Q.; Wan, Z.; Akgul, A.; Boyraz, O.F.; Yildiz, M.Z. Design and implementation of a new memristive chaotic system with application in touchless fingerprint encryption. *Chin. J. Phys.* **2020**, *67*, 615–630. [CrossRef]
24. García-Guerrero, E.; Inzunza-González, E.; López-Bonilla, O.; Cárdenas-Valdez, J.; Tlelo-Cuautle, E. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. *Chaos Solitons Fractals* **2020**, *133*, 109646. [CrossRef]
25. Chirakkarottu, S.; Mathew, S. A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography. *SN Appl. Sci.* **2020**, *2*, 1–10. [CrossRef]
26. Khan, A.; Jahanzaib, L.S.; Trikha, P. Changing dynamics of the first, second and third approximations of the exponential chaotic system and their application in secure communication using synchronization. *Int. J. Appl. Comput. Math.* **2021**, *7*, 1–26. [CrossRef]
27. El-Latif, A.A.A.; Abd-El-Atty, B.; Belazi, A.; Iliyasu, A.M. Efficient Chaos-Based Substitution-Box and Its Application to Image Encryption. *Electronics* **2021**, *10*, 1392. [CrossRef]
28. Abd-El-Atty, B.; Iliyasu, A.M.; Alaskar, H.; El-Latif, A.; Ahmed, A. A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. *Sensors* **2020**, *20*, 3108. [CrossRef]
29. True Color Kodak Images. Available online: http://r0k.us/graphics/kodak/ (accessed on 3 September 2021).
30. Alanezi, A.; Abd-El-Atty, B.; Kolivand, H.; El-Latif, A.; Ahmed, A.; El-Rahiem, A.; Sankar, S.; Khalifa, H.S. Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment. *Secur. Commun. Netw.* **2021**, *2021*. [CrossRef]
31. Xian, Y.; Wang, X. Fractal sorting matrix and its application on chaotic image encryption. *Inf. Sci.* **2021**, *547*, 1154–1169. [CrossRef]
32. Hua, Z.; Zhou, Y.; Huang, H. Cosine-transform-based chaotic system for image encryption. *Inf. Sci.* **2019**, *480*, 403–419. [CrossRef]
33. Abd el Latif, A.A.; Abd-el Atty, B.; Amin, M.; Iliyasu, A.M. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **2020**, *10*, 1–16.