mathematics

MDPI

Article

Modified SHARK Cipher and Duffing Map-Based Cryptosystem

Osama Rabie [1], Jawad Ahmad [2,*] and Daniyal Alghazzawi [1]

[1] Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 80200, Saudi Arabia; obrabie@kau.edu.sa (O.R.); dghazzawi@kau.edu.sa (D.A.)
[2] School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK
* Correspondence: j.ahmad@napier.ac.uk

Abstract: Recent years have seen a lot of interest in the study of chaotic structures and their accompanying cryptography frameworks. In this research, we came up with a new way to encrypt images that used the chaos and a modified block cipher named the SHARK cipher. The new algorithm looks at the creation of random sequences as a problem that needs to be solved in the best way possible, and then it uses the Duffing chaotic map to get even better random sequences. Chaos has been combined with a revised edition of the SHARK structure to make the algorithm design more robust with increased confusion and diffusion. The offered algorithm includes a complex encryption and decryption structure with minimal time consumption for secure data transmission. The proposed algorithm is verified with the encryption of some standard images of different sizes. Numerous analyses have been performed to see how well the algorithm works against a variety of assaults, and the outcomes show that the cryptosystem has a good level of robustness. The comparative results are also performed in this work, which guarantees the excellent performance of our cryptosystem. The system is also subjected to chosen-plaintext and chosen-ciphertext attacks which implies that it can resist many classical cryptographic attacks. Therefore, our cryptosystem is robust enough to use for image encryption.

Keywords: SHARK; chaos; duffing map; image encryption; modified algorithm

MSC: 65P20

check for updates

Citation: Rabie, O.; Ahmad, J.; Alghazzawi, D. Modified SHARK Cipher and Duffing Map-Based Cryptosystem. *Mathematics* **2022**, *10*, 2034. https://doi.org/10.3390/math10122034

Academic Editor: Lingfeng Liu

Received: 26 May 2022
Accepted: 8 June 2022
Published: 12 June 2022

1. Introduction

The transmission of personal data utilizing the internet has increased substantially in the current era with the expansion of information technology into practically every sector. Nasty and unapproved approach efforts to personal and private data are becoming more tempting as the volume of crucial information being transmitted over this medium grows daily. Maintaining digital data security continues to be a challenge. Network-based biometric verification has become commonplace in today's environment, where image data of biometric signals such as fingerprint or iris scans must be securely sent.

To guarantee data confidentiality, integrity, non-repudiation, and authentication, encryption is used. It ensures safe communication from end to end. Encryption's core notion is to safeguard plaintext data such that it can only be deciphered by a legitimate receiver with the right secret key. The classical Shannon requirements of diffusion and confusion must be met by a strong encryption method with good statistical characteristics, as well as being resistant to cryptographic assaults. As much as possible, the ciphertext and private key connection should be made as ambiguous as possible, while diffusion reshuffles bits of the plaintext such that any dismissal in the plaintext is dispersed throughout the ciphertext to make the ciphertext more secure. Traditional encryption methods such as AES [1], DES [2], RSA [3], and so on are available. Text data can be encrypted well using these approaches, but the number-theory-based encryption methods are not well-suited for multimedia data. There is a significant degree of correlation between neighboring pixels/frames in multimedia data, as well as spatial and temporal redundancy. For real-time multimedia applications, such as satellite communication, video conferencing, image-based military, image surveillance, etc., typical encryption methods require a lot of processing power, a long computation time, and a lot of money. As a result, improved solutions are needed to address multimedia data security concerns. Image data, unlike traditional textual information, has several essential and inherent properties: There is a strong connection between nearby pixels and there is a lot of data redundancy. These factors necessitate the development of innovative algorithms that vary from traditional block cipher algorithms built specifically for text data, such as DES and AES.

In several ways, chaotic signals resemble cryptographic properties such as (1) the ergodicity property, (2) the high sensitivity of chaotic signals to their initial conditions/system parameters, and (3) the noise-like behavior of chaotic sequences, all of which can be compared to the properties of cryptographic key sequences. Chaotic systems are very unpredictable and random because of their highly sensitive reaction to beginning circumstances. As a result, the creation of discrete chaos signals utilizing chaotic systems is generally cost-effective. How to create ways for encrypting multimedia data using chaos-based encryption is now being studied by researchers and academics. The security weaknesses in some of these systems mean they cannot survive even the most basic of cryptographic assaults, as several cryptanalysts have demonstrated.

1.1. Literature Review

A chaos-based PRNG (Pseudorandom number generator) encryption scheme provides maximum randomness to the cipher image. Therefore, we have reviewed some chaos-based encryption schemes to check the robustness of the existing work. Color images can be encrypted by applying a chaotic logistic map and permutation-diffusion approach developed by Pareek et al. [4]. Using the MD5 value of the original image, Gao et al. [5] constructed an encryption technique for images, established based on chaos theory. Using two chaotic maps, Wang et al. [6] recommended an encryption procedure created on the SHA-3 algorithm and the one-time pad effect. A two-dimensional sine logistic modulation map presented by Hua et al. [7] was based on logistic and sine maps. A novel two-dimensional chaotic system was developed by Zhu et al. [8] employing logistic and sine maps. A new 2D sine map (2D-SM) with a straightforward algebraic composition was presented by Bao et al. [9]. Gao suggested an improved Henon map (IHM) color image encryption technique [10]. El Assad and Farajallah [11] suggested a 2D cat-map-based image encryption system that includes a diffusion layer as well as a bit-permutation layer. Li et al. [12] introduced an innovative cryptosystem constructed on the tent chaotic map, which had previously been demonstrated to be effective. Zhang and Wang [13] introduced a novel multiple-image encryption technique constructed on the piecewise linear map and mixed image element, which is a relatively fast method of encrypting, and similar. However, due to the simplistic nature of the applied chaotic maps, certain current techniques have been proven to represent security risks [14]. Using different combinations of these eminent chaotic maps, as well as other mathematical manipulations [15–18], researchers attempted to build image encryption techniques. Image encryption was proposed by Lio and Maio [19] by altering the parameters of a logistic map. Resistance to phase space reconstruction can be achieved using a 2D logistic map for encryption, shoqn by Wu et al. Differential assaults cannot get in the way of this strategy. Chaotic image encryption using secure hash algorithm-3 was proposed by Ye and Huang [20]. There was a combination of permutation and diffusion employed in this experiment. For image encryption, Lian et al. [21] used a spatiotemporal chaotic system. The security of their algorithm is greater at a lower cost. Preprocessing the image encryption was proposed by Ye and Huang [22] as a modular operation. Keystreams are generated using a self-adaptive encryption technique. Unlike Fridrich, Ye et al. [23] devised an image encryption method that incorporates modulation, permutation, and diffusion. Entropy was employed to generate the keys. Solak et al. [24] also evaluated Fridrich's chaotic encryption technique, which was introduced by Solak and colleagues. There is a new way to challenge Fridrich's technique that has been offered by Xie et al. A cosine transform-based image encryption technique was developed by Hua et al. [25]. Kumar et al. [26] offered a new image encryption scheme with Zig Zag scan-based convolution and enhanced thorp shuffle. Authors in [27] presented an innovative encryption structure based on the Lorenz chaotic map and utilized the random sequences by a switch control mechanism to ensure robustness. Li et al. [28] proposed a novel encryption scheme based on plaintext-dependent permutation and DNA encoding. Arif et al. [29] suggested a novel encryption structure based on permutation and substitution using the Logistic map and random replacement. Pixels are scrambled using chaotic techniques. The encrypted image is greatly affected by even the smallest changes to an image [30–35].

1.2. Contribution

The major involvement of chaos in cryptography leads to innovative ideas to boost the encryption execution of traditional block ciphers with a mixture of chaotic maps. The key impacts of this work are as follows:

1. Introducing an efficient cryptosystem based on a mix of chaos and a modified SHARK cipher encryption.
2. The proposed system uses a structure of SPN with plaintext-dependent random keys generated from the duffing chaotic map.
3. The technique employs numerous phases to achieve extremely random sequencing with minimal correlation.
4. Examining and comparing several present state-of-the-art procedures with the offered cryptosystem.
5. The proposed scheme is investigated thoroughly using various tests, i.e., histogram, information entropy, peak signal to noise ratio (PSNR), mean squared error (MSE), unified average changing intensity (*UACI*), number of pixels changing rate (*NPCR*), National Institute of Standard and Technology (NIST), chi-square analysis, correlation coefficient, and computational complexity analysis.

The rest of the manuscript is ordered as follows: Section 2 offers a brief overview of the modified SHARK cipher, Section 3 includes a proposed encryption scheme, performance analyses of the offered encryption technique are presented in Section 4, and Section 5 depicts a comparative analysis of the offered scheme with, finally, a conclusion being drawn.

2. Modified SHARK Algorithm

The SHARK cipher was suggested by Rijmen et al. [30] in 1996. The algorithm comprises the structure of SP networks. The SHARK cipher comprises a non-Feistel structure with some weaknesses in the secret keys. The basic structure of the SHARK cipher was comprised following main points:

Confusion Layer.
Diffusion Layer.
Key generation for each round.

A strong cipher is built by considering each construction component independently. We choose a diffusion layer that is consistent and has excellent diffusion qualities. As the nonlinear layer has even nonlinear characteristics, we do not have to consider the intricacies of the interface among the nonlinear and the diffusion layer when gauging the cipher's resistance to cryptanalysis. When the S-boxes are replaced with other S-boxes with equal nonlinearity qualities, the cipher's resistance stays unchanged. This is a variation on the wide trail technique [30]. Since each structure block is chosen and assessed independently, it is not sought to compensate for non-linear layer shortcomings with extra linear layer qualities.

By taking the vulnerabilities of the original cipher into account, the algorithm was cryptanalyzed by Jakobsen and Knudsen [31] in 1997 by interpolation attack. In this research, we have modified the SHARK algorithm eliminating the vulnerabilities in the original structure. The improved structure includes 10 rounds of encryption with the secret keys utterly dependent on the input inserted in the algorithm. The robustness of the modified algorithm is increased by inserting the data obtained from the 9th round through the conditional algorithm. The vulnerabilities in each building block are reduced by the accumulation of input-dependent secret keys. The design strategy of the modified cipher includes the following structure.

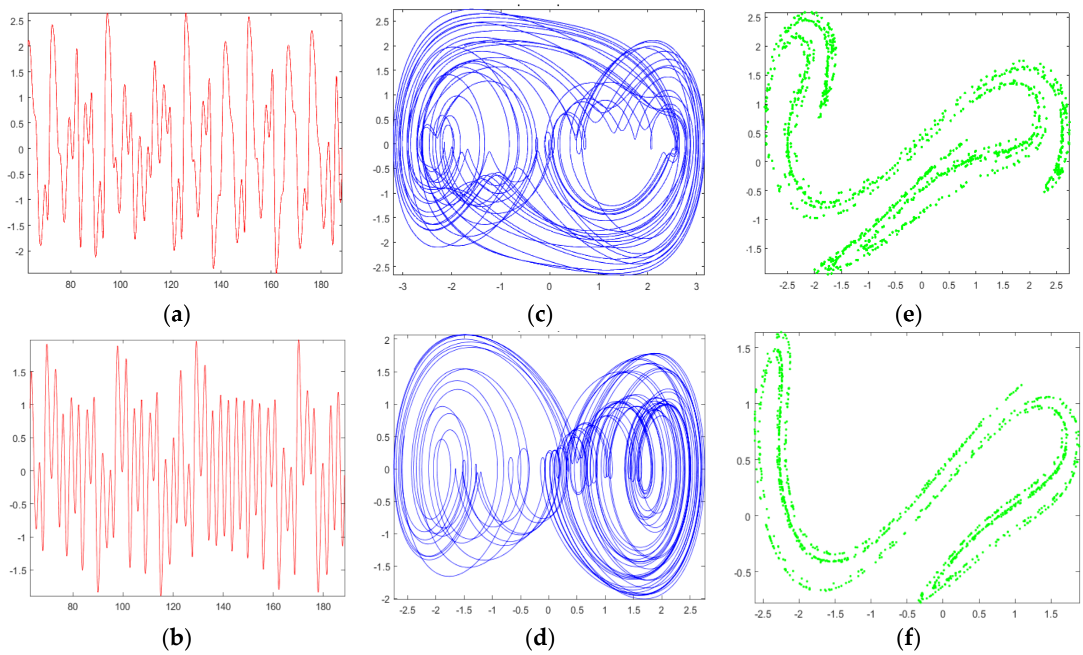
The first improvement in the SHARK cipher is made by increasing the input bit space from 64-bits to 128-bits. The encryption algorithm takes 128-bit plaintext as an initial seed. The next segment of the algorithm is distributed into two phases. The first segment comprises nine rounds with similar operations. Then conditional diffusion is applied to the 9th round cipher data. Then, the output is transferred to the second phase which is the 10th round of the encryption technique.

3. Offered Encryption Algorithm

The proposed encryption model comprises the key generation structure through a chaotic duffing map. The chaotic duffing system is a discrete-time dynamical structure. It is an illustration of a chaotic system that reveals chaotic performance. The duffing map gets the input points (x_n, y_n) in the plane and maps them into a different point presented by

$$\begin{cases} x_{n+1} = y_n \\ y_{n+1} = -bx_n + ay_n - y_n^3 \end{cases} \tag{1}$$

The behavior of the chaotic map may vary concerning the change in the initial conditions and parameters. Therefore, the behavior of a chaotic map is determined by taking two different sets of parameters and initial conditions for the set (1) and performing a time-series plot, phase space plot, and Poincare diagram. The randomness visual assessment of the chaotic duffing map is shown in Figure 1. The result in the depicted figure explains the large variation in the visual plot with a trivial variation in the parameters, which leads to the sensitivity of the chaotic map.



(**a**) (**c**) (**e**)

(**b**) (**d**) (**f**)

Figure 1. Chaotic Duffing map with two different sets of parameters. (**a**,**b**) Times series plots, (**c**,**d**) Phase space plots; (**e**,**f**) Poincare diagram.

The randomness of the chaotic sequences can also be measured by using the NIST test suite 800-22. The outcomes of the binary sequences are depicted in Table 1. p values of the X, Y, and Z components show that the sequences generated from the chaotic duffing map are highly random with no periodicity. Hence, we can say that the duffing map can be utilized in the proposed cryptosystem to generate highly random keys.

Table 1. NIST randomness measure for Duffing map chaotic sequences. $\surd$ means test is passed.

	***p* Values for Each Chaotic Sequences**			**Status**
Analysis	**X**	**Y**	**Z**	
Frequency	0.1153	0.5961	0.1174	$\surd$
Block-frequency	0.9631	0.8963	0.9654	$\surd$
Runs	0.6884	0.1547	0.0947	$\surd$
Universal	0.9974	0.5187	0.3349	$\surd$
Block-frequency	0.0101	0.9962	0.8585	$\surd$
Overlapping	0.8114	0.8114	0.8114	$\surd$
Spectral DFT	0.0114	0.4477	0.1593	$\surd$
No overlapping	0.8962	0.7954	0.7426	$\surd$
Universal	0.9901	0.9987	0.9963	$\surd$
Cumulative sums forward	0.0036	0.0147	0.0852	$\surd$
Approximate entropy	0.5253	0.4468	0.8991	$\surd$
Cumulative sums reverse	0.7845	0.6650	0.6701	$\surd$

3.1. Key Generation

The robustness of the encryption structure entirely varies on the private key of the cryptosystem. In the late 19th century, Dutch cryptographer Auguste Kerckhoff's postulate became famous as the Kerckhoff Principle, "a cryptosystem should be secure even if everything about the system, except the key, is public knowledge". Therefore, the key generation of the system must be robust to resist all possible cryptographic attacks. By taking this principle into account, we have developed the secret keys of the system from the input of the algorithm which changes with each input. The initial seeds for the duffing map can be determined by:

$$x_0 = \frac{\sum_{i=1}^{n} P_i^R}{M \times N} \tag{2}$$

$$y_0 = \frac{\sum_{i=1}^{n} P_i^C}{M \times N} \tag{3}$$

where P_i^R signifies the rows of the original data matrix P, P_i^C denotes all the columns of the plain data matrix P, and $M \times N$ is the dimensions of the input image.

3.2. Encryption Procedure

This approach employs image diffusion and replacement encryption constructed on chaos to thoroughly optimize the algorithm's security and efficiency. In addition, the image content relates to the equivalent key. Our proposed encryption algorithm as shown in Figure 2 utilizes the initial keys of the duffing map generated from the previous step. The main procedure of the encryption is partitioned into two components: the first component is the execution of the duffing map, and the second part is the modification of the SHARK algorithm. The working strides of the suggested encryption system are as follows:

Step 1 The data matrix of the plaintext image is signified by P, and it is read to be encrypted. The image size, which is the number of pixel rows M and the number of pixel columns N, is obtained. There are M pixels in the first row and N pixels in the first column, hence P is equal to the sum of these values, $P = \{p(i,\ j)\}$, i = 1, 2, . . . , M; j = 1, 2, . . . , N.

Step 2 The initial keys of the duffing map are constructed by seeding the input image in Equations (1) and (2). Then after getting x_0, y_0 the private keys of the encryption algorithm are generated from the duffing map.

Step 3 The modified SHARK algorithm with the SPN (Substitution Permutation Network) structure is applied to the input data. The first $(n-1)$ rounds are kept the same as the original SHARK cipher with a different encryption key.

Step 4 Before the last round of the modified SHARK cipher, a conditional diffusion algorithm is applied as:

$$\begin{cases} \text{If } mod\left(sum\left(E^{n-1}\right), 256\right) < 128, \text{ then } E^{n-1} \oplus K_s, \\ \qquad\qquad\qquad\text{else}, \ E^{n-1} \oplus K_p. \end{cases} \tag{4}$$

where E^{n-1} is the encrypted matrix obtained after $(n-1)$ rounds of the modified SHARK cipher, and K_s and K_p are the substitution and permutation keys of the system, respectively.

Step 5 The last round of the SHARK cipher is applied on the cipher image obtained from step 4 and then complied as the encrypted image.

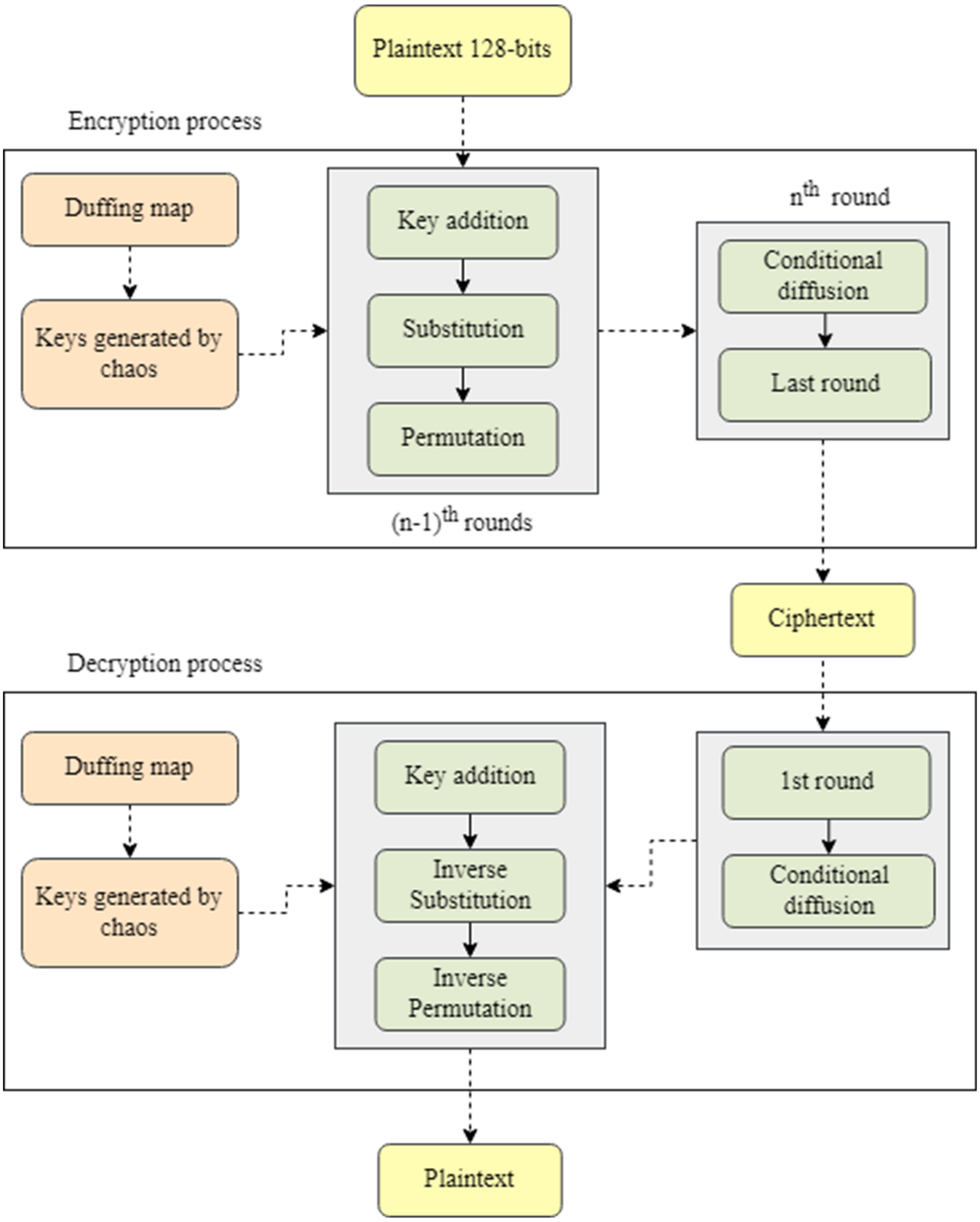


Figure 2. Flow chart illustration of modified SHARK cipher-based encryption algorithm.

3.3. Decryption Procedure

The decryption of the offered encryption method involves the same steps in a reverse manner. The decryption strides are as follows:

Step 1 The inverse of the last round of SHARK cipher is applied to the encrypted image, which includes inverse permutations, inverse substitution, and key XOR.

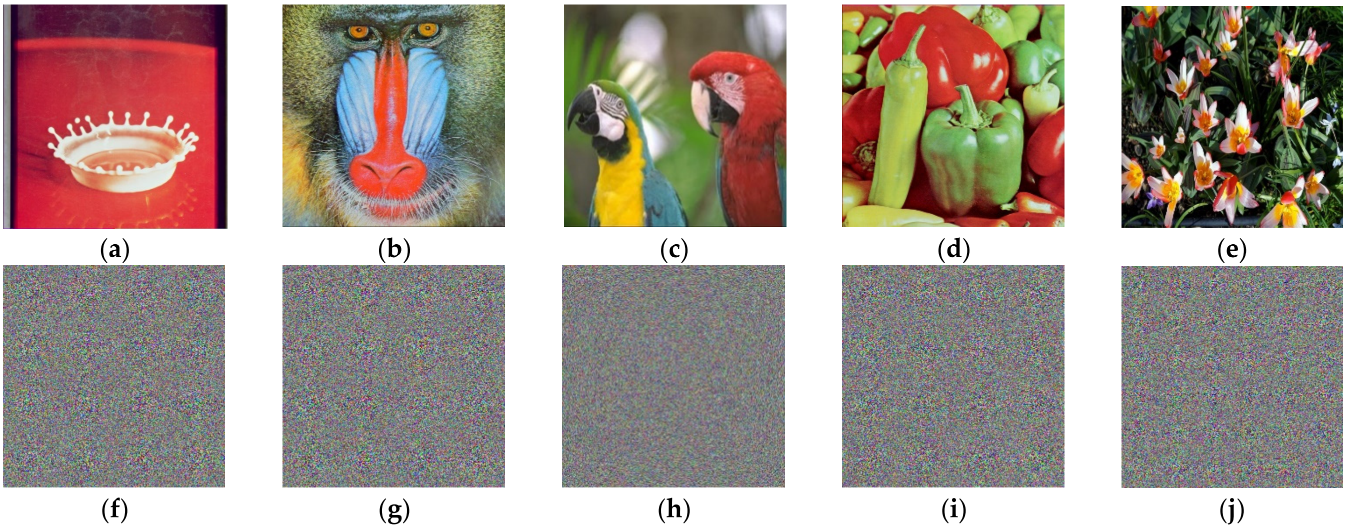
Step 2 The image data obtained from step 1 is then passed from the conditional shift algorithm in which the key used for encryption is utilized to decrypt whether it is K_s or K_p, where the selection of these keys is entirely made by using Equation (4).

Step 3 The next $(n-1)$ rounds are implemented on the image attained from step 2. The inverse of each operation, permutation, substitution, and key addition are utilized for $(n-1)$ times to get the original data.

The final data obtained after the implementation of the inverse modified SHARK algorithm is then compiled as original image data.

4. Security Analysis and Numerical Results

The experiments are performed on a Microsoft Windows 10 OS with an Intel (R) Core (TM) i5-9300HF, 8 GB of RAM, 2.4 GHz processor. We utilize MATLAB 2020 to implement encryption and decryption algorithms. The investigational images are selected from the USC-SIPI image databases. Different images of Splash, Baboon, Peppers, Tulips with dimensions 512 × 512 × 3, and Parrots with dimensions 256 × 256 × 3 are utilized as original images. The outcomes of the enciphered images are shown in Figure 3.



(**a**) (**b**) (**c**) (**d**) (**e**)

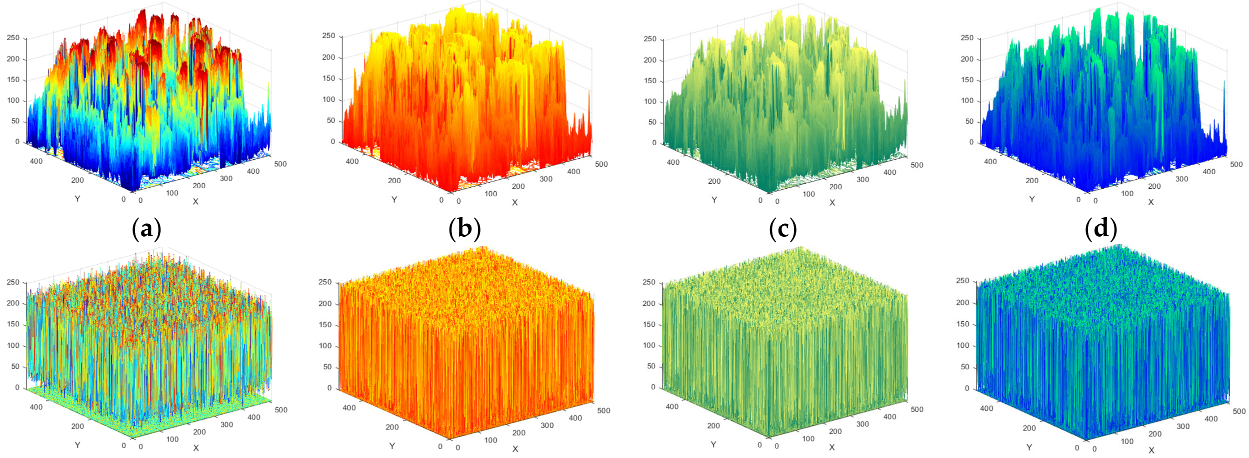
(**f**) (**g**) (**h**) (**i**) (**j**)

Figure 3. (**a**–**e**) Original standard color images; (**f**–**j**) respective ciphers yielded by the offered scheme.

To certify the quality of the offered encryption algorithm we have executed some standard statistical analyses. Visual analyses include a histogram, correlation, occlusion attack, and numerical analyses including a correlation coefficient, entropy, peak signal to noise ratio (PSNR), mean square error (MSE), number of pixels changing rate (*NPCR*), unified average changing intensity (*UACI*), NIST, computational complexity, and keyspace analysis.

4.1. Histogram Analysis

Histograms are used to illustrate the association between the value of the pixel and the frequency of each pixel value in an image. Gray-level and color images of size $N \times M$ with $N = H$ and then $N \times M$ are used to test and examine the cryptosystem. The 3D histograms of the Tulip image with a size of 256 × 256 × 3 are depicted in Figure 4. The histogram for both plain and ciphered images is displayed for each image. Figure 4 shows that simple image histograms have various modes representing distinct regions, whereas enciphered image histograms are uniform. This is a fantastic sign of the proposed cryptosystem's excellent encrypting procedure.



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

(**e**) (**f**) (**g**) (**h**)

Figure 4. (**a**–**d**) Three dimensional histograms of the original Tulip image layers; (**e**–**h**) respective 3D histograms of cipher image layers.

4.2. Correlation

Correlation analysis describes the association among two nearby pixels in an image. An assailant can use a high correlation between adjoining pixels in the enciphered data image to figure out the association among the plain data image and the ciphered image. Accordingly, to assess the scheme's security, a correlation analysis of two neighboring pixels is required. From the original and ciphered images, we randomly picked 10,000 sets of two neighboring pixels in horizontal, vertical, and diagonal axes, and computed the coefficient of all sets using Equation (5).

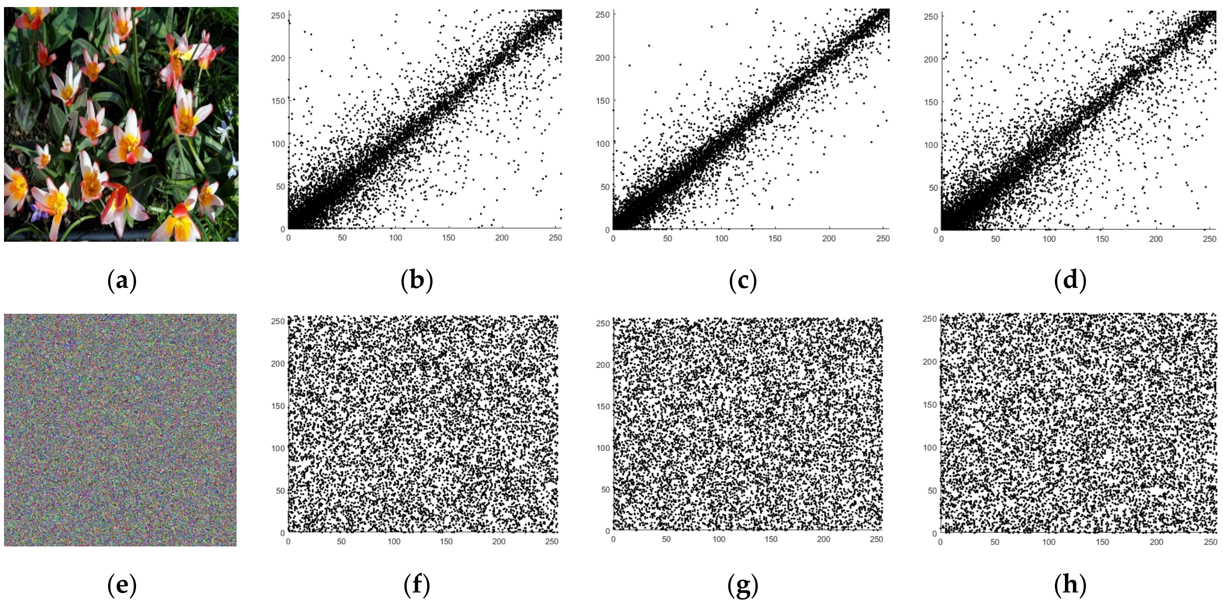
$$Cr = \frac{K \times \sum_{i=1}^{K} X_i Y_i - \sum_{i=1}^{K} X_i^2 \times \sum_{i=1}^{K} Y_i^2}{\sqrt{\left(K \times \sum_{i=1}^{k} (X_i)^2 - \left(\sum_{i=1}^{K} X_i\right)^2\right) \times \left(N \times \sum_{i=1}^{K} (Y_i)^2 - \left(\sum_{i=1}^{K} Y_i\right)^2\right)}} \tag{5}$$

where X and Y are the greyscale estimates of two neighboring pixels, and K denotes the total of pairings. Cr is the correlation value, and it falls inside the [1, 1] range. $Cr \to 0$ denotes a very low correlation, while $Cr \to 1$ denotes a very strong correlation. Table 2 indicates the results of our ciphered image correlation that are closer to 0.

Table 2. Correlation Coefficient results for different images.

	Original Image			**Enciphered Image**		
Image	**Horizontal**	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Splash	0.9674	0.9559	0.9793	0.0002	0.0090	−0.0010
Baboon	0.9514	0.9221	0.8704	−0.0014	−0.0038	0.0007
Parrots	0.9985	0.9561	0.8991	−0.0016	−0.0009	−0.0027
Peppers	0.8974	0.7354	0.6358	−0.0008	0.0015	−0.0011
Tulips	0.9325	0.7892	0.8967	0.0010	−0.0011	−0.0138

In addition, Figure 5a–d depict the horizontal, vertical, and diagonal correlation dispersals for the Tulips' original image, whereas Figure 5e–h depict the horizontal, vertical, and diagonal correlation distributions for the Tulips' enciphered image. This correlation study demonstrates that the encryption technique has no statistically significant flaws.



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

(**e**) (**f**) (**g**) (**h**)

Figure 5. (**a**) Plain Tulips image; (**b**–**d**) correlation diagram of plain Tulip image in horizontal, diagonal, and vertical axes, correspondingly; (**e**) encrypted Tulips image; (**f**–**h**) correlation diagram of encrypted Tulip image in horizontal, diagonal, and vertical axes, correspondingly.

4.3. Entropy

Entropy is an assessment of the degree of unpredictability in the image information. It is utilized to evaluate the uncertainty of the suggested algorithm. The information entropy of an image is executed to verify the randomness of its dissemination of grey pixel values. According to Shannon's theory, it is determined as the following mathematical expression:

$$H(m) = \sum_{i=1}^{M} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{6}$$

where $p(m_i)$ signifies the probability of the existence of sign m and M signifies the total bits for every sign m because a grayscale image has 256 pixels and the data points of the pixels have 28 probable sequences, meaning the entropy value of a randomly enciphered image is eight, in theory. Table 3 displays the entropy values of the enciphered Splash, Baboon, Parrots, Peppers, and Tulips images. Since each number is slightly above 7.99, it may be concluded that a given encryption structure randomizes the dispersal of the pixels in the original image, making it difficult for an assailant to learn anything from its encrypted form.

Table 3. Entropy analysis for different standard image layers.

Image	Layers	Original	Encrypted
Splash	Red	6.9481	7.9986
	Green	6.8845	7.9991
	Blue	6.1265	7.9998
Baboon	Red	7.7379	7.9989
	Green	7.4608	7.9994
	Blue	7.7683	7.9998
Parrots	Red	7.5458	7.9999
	Green	7.5669	7.9987
	Blue	7.3757	7.9998

Table 3. *Cont.*

Image	Layers	Original	Encrypted
Peppers	Red	7.3388	7.9997
	Green	7.4963	7.9988
	Blue	7.0583	7.9996
Tulips	Red	7.4734	7.9991
	Green	7.6001	7.9978
	Blue	6.8581	7.9997

4.4. Ciphertext Sensitivity Analysis

Decryption systems can alter the plaintext image in ciphertext sensitivity analysis to see how the restored plaintext image differs from the original plaintext image. A system's ciphertext sensitivity is said to be strong when the decrypted image differs substantially from the original plaintext image; on the other hand, a system's ciphertext sensitivity is said to be weak if the restored image does not differ much from the original plaintext image. One or more pixels in each ciphertext picture can be changed to reflect slight changes in the ciphertext image. Different plaintext photos P were chosen for this work, and this encryption scheme was used to acquire the associated ciphertext image C_1. Decrypting C_2 resulted in P_1 as the decrypted version of C_2; a random pixel point from C_1 was selected and its value was altered by one. The mathematical expression of $NPCR$ and $UACI$ is defined as:

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j)}{w \times h} \tag{7}$$

$$UACI = \left[\frac{\sum_{i=1}^{w} \sum_{j=1}^{h} \left| C_{1(i,j) - C_2(i,j)} \right|}{(2^8 - 1) \times w \times h} \right] \times 100\% \tag{8}$$

where w and h indicate image dimensions and i, j denote the pixel position of the image.

Table 4 shows the computed estimates of $NPCR$ and $UACI$ for P and P_1. Table 4 indicates that the determined $NPCR$ and $UACI$ estimates are close to their theoretical standards, indicating that the encryption system has an elevated ciphertext sensitivity.

Table 4. *NPCR* and *UACI* measures for various standard images.

Test	Image	Result
NPCR	Splash	99.6374
	Baboon	99.5815
	Parrots	99.6016
	Peppers	99.6125
	Tulips	99.5925
UACI	Splash	33.3478
	Baboon	33.1709
	Parrots	33.8935
	Peppers	33.0369
	Tulips	33.5048

4.5. Mean Squared Error and Peak Signal to Noise Ratio

The suggested scheme's dependability is assessed using the mean squared error (MSE). To find any similarities or differences between plain and encrypted photos, it is analyzed by looking at the pixels of both images side by side. It can be stated numerically as follows:

$$\text{MSE} = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(P_{ij} - E_{ij}\right)^2}{M \times N} \tag{9}$$

where P_{ij} is a pixel from the plain image and E_{ij} is a pixel from the encrypted image. The total number of pixels in any of the photos is given by the product $M \times N$. In theory, the value of the MSE must be larger to create a system that is resistant to statistical assaults. The quality of the enciphered image is also evaluated by PSNR analysis. This is a ratio of the image's greatest pixel value to the MSE. It is mathematically represented as

$$\text{PSNR} = 10 \log \left(\frac{I_{max}^2}{\text{MSE}} \right) \tag{10}$$

where I_{max} is the maximum pixel value (255). As the PSNR is inversely associated with the MSE, the theoretical value should be as low as feasible. The lower the PSNR readings, the higher the indicator of the encryption scheme's quality. Values of PSNR and MSE are shown in Table 5.

Table 5. MSE and PSNR analysis for some standard image layers.

Image	Layers	MSE	PSNR
Splash	Red	8096.03	7.8521
	Green	11,141.62	9.5126
	Blue	9110.45	8.5963
Baboon	Red	9099.58	7.6363
	Green	7048.36	7.5541
	Blue	8948.70	7.6999
Parrots	Red	9945.10	8.9597
	Green	10,635.56	8.9632
	Blue	8267.22	9.6358
Peppers	Red	8578.69	8.9657
	Green	7995.11	7.5294
	Blue	8328.01	8.4007
Tulips	Red	9336.17	9.1148
	Green	11,014.77	9.6557
	Blue	10,478.50	7.0041

4.6. NIST

The NIST analysis suite includes several randomness tests that must be met by a competent PRNG. Each of the tests must have a p-value larger than 0.01 to be considered random in the context of the bitstream. In the NIST set of tests, across many long bit sequences, the suggested encryption technique passes all of them. For example, Table 6 provides a breakdown of the findings of the NIST study of the encrypted Tulip image's color channels. The suggested image-encryption technique passed the NIST examination, as the results for all the tests were more than 0.01.

Table 6. NIST randomness measure for Tulip encrypted image. $\surd$ means test is passed.

	p **Values for Each Layer of the Enciphered Image**			**Status**
Analysis	**R**	**G**	**B**	
Frequency	0.0035	0.2563	0.0745	$\surd$
Block-frequency	0.0895	0.0579	0.3405	$\surd$
Runs	0.7985	0.1029	0.3636	$\surd$
Long runs of ones	0.0357	0.0357	0.0357	$\surd$
Universal	0.9952	0.9978	0.9951	$\surd$
Block-frequency	0.0895	0.0579	0.3405	$\surd$
Overlapping	0.8114	0.8114	0.8114	$\surd$
Rank	0.2919	0.2919	0.2919	$\surd$

Table 6. *Cont.*

	***p* Values for Each Layer of the Enciphered Image**			**Status**
Analysis	**R**	**G**	**B**	
Spectral DFT	0.9383	0.0014	0.5742	√
No overlapping	0.9963	0.9810	0.9983	√
Universal	0.9952	0.9978	0.9951	√
Cumulative sums forward	0.0369	0.2099	0.2274	√
Approximate entropy	0.9630	0.9547	0.8770	√
Cumulative sums reverse	0.8911	0.6010	0.8312	√

4.7. Security against Brute Force Attack

Typically, the security key of chaos-based cryptography contains two main components, which are the control parameters and initial conditions of the employed chaotic map. In the suggested encryption technique, the parameters and initial conditions of the enhanced duffing map (4) are employed as the main root of public and private keys. Each parameter and initial value takes 15 to 16 decimal places, which means that the complexity of each parameter and the initial value is 2^{52}. In addition to that, the chaotic sequences of the duffing map (4) are generated by the parameters and initial conditions for constructing the permutation and substitution keys for the modified SHARK cipher. Therefore, the keyspace in producing permutation and substitution keys is $2^{2(128)}$ (for 128* bit operation) $\times 2^{52}$ initial conditions/ = 2^{308}, and the total key combinations are 2^{128}, i.e., the key size in this proposed algorithm is 128 bits. Therefore, the security key of the suggested algorithm is 2^{436} which achieves the standard requirement. The keyspace of the offered cryptosystem is substantial enough to defeat all the classical attacks and brute force assaults.

4.8. Cropped Attack

Simulations of occluded encrypted data have been run to determine if the proposed approach can withstand the loss of encrypted data. Perceptual image quality and numerical analysis are used to describe these simulations' outcomes. To run simulations, we occluded 1/2, 1/4, 1/16, and 1/64 of the data in the enciphered image, as displayed in Figure 6. As noticed in Figure 6a–d, the encrypted image contains 1/64-part, 1/16-part, 1/4-part, and 1/2-part occluded data. Figure 6e–h show the reconstructed pictures. The images that were recovered using the right keys are what were expected. Digital post-processing can enhance the quality of recovered images. The suggested approach is resistant to distortion caused by the loss of encrypted data since the input image pixels are distributed uniformly in the encrypted output. Images may be sent over networks with a lot of traffic using the offered algorithm.

4.9. Execution Time Analysis

The execution time is the amount of time necessary to transform the text into an image algorithm. It is the total of the compile and run times. For the effective implementation of text-to-image encryption, the execution time should be kept to a minimum. It is commonly expressed in seconds, milliseconds, or minutes. The execution time for different sizes of image insertion into the proposed algorithm is shown in Table 7. Table 7 expresses that the proposed approach is extremely quick, with processing times.

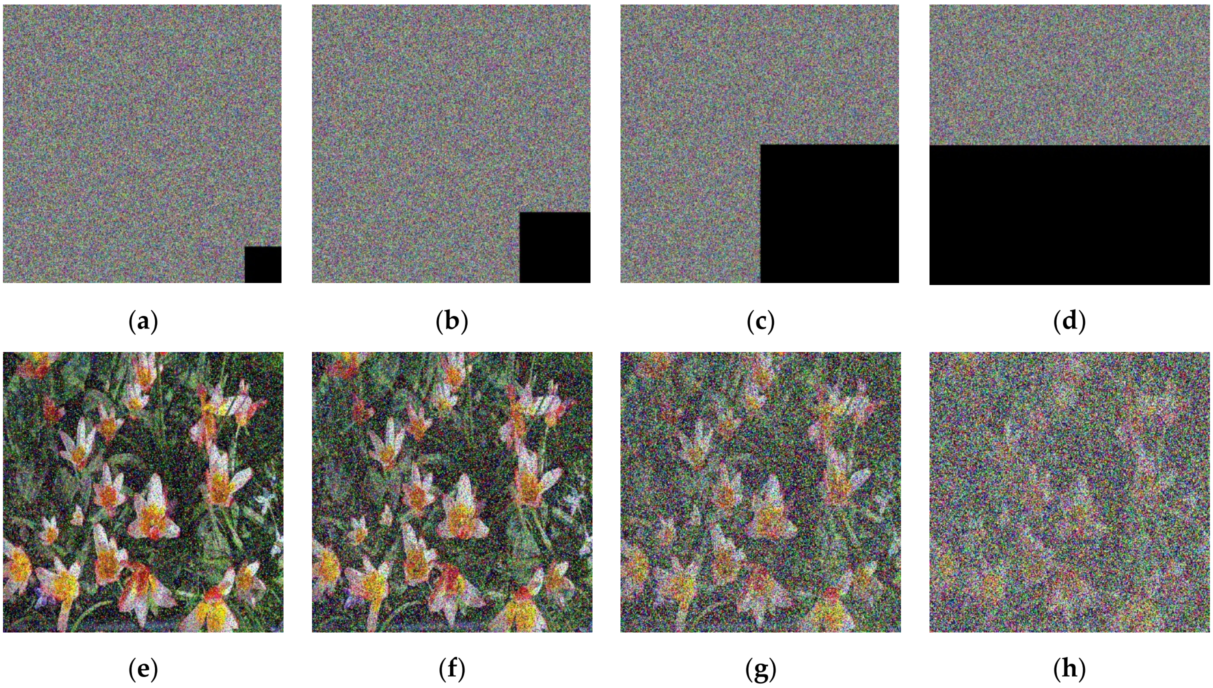


Figure 6. Enciphered and deciphered images after (**a**) 1/64 occlusion; (**b**) 1/16 occlusion; (**c**) 1/4 occlusion; (**d**) 1/2 occlusion; (**e**) deciphered image after 1/64 occlusion; (**f**) deciphered image after 1/16 occlusion; (**g**) deciphered image after 1/4 occlusion; (**h**) deciphered image after 1/2 occlusion.

Table 7. Execution time (in seconds) of the proposed cryptosystem.

Image Size	Execution Time
128 × 128 × 3	0.5211
256 × 256 × 3	1.0084
512 × 512 × 3	2.9961
1024 × 1024 × 3	5.0018

4.10. Classical Cryptanalysis Attacks

A possibility of the cryptanalysis of the offered scheme by using some classical attacks exists. Therefore, if we subject the system to the chosen-plaintext/chosen-ciphertext attack, the assailant may get some temporary access to the encryption device. Even if the attacker inserts some chosen plain or encrypted data, acquiring the secret key is still complicated because the private key changes with the change of each input data. Additionally, the offered algorithm produces a cipher that does not reveal any relationship between the private key and plaintext. Even if the attacker inserts a full black or full bright image with all the same pixel values, he cannot get any proper information about the key. Therefore, we can declare that our offered encryption structure is secure against classical cryptanalysis attacks.

5. Comparative Analysis

The offered encryption algorithm is subjected to comparative analyses with some recently publish schemes. The keyspace, *NPCR*, *UACI*, entropy, MSE, PSNR, and correlation measures are compared with Refs. [32–35]. Table 8 presents the comparative results performed for the Peppers image with the dimensions 256 × 256 × 3. The keyspace of the suggested encryptions technique is robust, as compared to the existing literature. The *NPCR* and *UACI* measures of the offered scheme are much closer to ideal values, in contrast to the other standard work. The table below illustrates the entropy value of the encrypted image, as well as how they evaluate to attain standards in the literature. The attained entropies are all slightly higher than 7.99, which is quite near to the optimum entropy value of eight and comparable to the literature. Table 8 compares the estimated MSE values for the encrypted image with those of other techniques from the literature. The MSE value calculated for encrypted images using the proposed approach is equivalent to or better than those obtained from other systems in the literature. Table 8 compares the calculated PSNR value for the encrypted image to those of other techniques from the literature. The PSNR estimated for the enciphered images using the proposed approach are equivalent to or better than those acquired from previous techniques in the literature.

Table 8. The contrast of statistical calculations of the suggested method with existing work.

Analysis	**Proposed**	**Ref. [32]**	**Ref. [33]**	**Ref. [34]**	**Ref. [35]**
Keyspace	2^{436}	2^{425}	2^{430}	-	10^{112}
NPCR	99.612	99.59360	99.60937	99.63	99.5174
UACI	33.063	32.17523	33.83490	30.51	33.4682
Entropy	7.9993	7.99877	7.99890	7.95264	7.9965
MSE	8300.6	10,092.3	-	-	10,869.73
PSNR	8.2986	8.09089	-	-	7.7677
			Correlation		
Horizontal	0.0015	−0.00063	−0.0020	0.0040	−0.0015
Diagonal	−0.0008	−0.00003	0.00008	−0.0016	0.0037
Vertical	−0.0011	−0.00102	−0.0064	−0.0015	0.0030

6. Conclusions and Future Recommendations

Shannon's principles of diffusion and confusion are used in this work to develop an RGB image encryption system. Three steps are involved in the implementation of the proposed strategy. The first step includes the key generation for the duffing map using the rules defined in Equations (3) and (4). The second step includes the construction of diffusion, and S-box and P-box keys. Finally, the modified SHARK cipher structure is implemented with the generated keys as offered by the encryption algorithm in the third step. The scheme's performance was assessed using a variety of statistical and differential indicators. An MSE analysis, correlation coefficient analysis, PSNR, information entropy, a computational complexity analysis, a differential assault evaluation (in terms of *UACI* and *NPCR*), a keyspace analysis, cropped attack, and a NIST analysis were among the techniques used. According to the calculations, the suggested technique is resilient to statistical, differential, and brute-force assaults. Furthermore, when contrasted to other image encryption structures in the literature, the suggested color image encryption method demonstrated either an equivalent or greater robustness performance.

The offered work can also be extended to the encryption of audio and video data. Moreover, using the strategy of key generation by the chaotic algorithm and conditional diffusion, one can also modify the other block ciphers with weak structures.

Author Contributions: Conceptualization, O.R., J.A. and D.A.; Data curation, J.A.; Formal analysis, O.R. and D.A.; Investigation, D.A.; Resources, J.A.; Supervision, J.A. and D.A.; Validation, O.R.; Writing—original draft, O.R. and J.A. All authors have read and agreed to the published version of the manuscript.

Funding: The Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia has funded this project, under grant no. (RG-10-611-43).

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

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

References

1. Advanced Encryption Standard (AES). Federal Information Processing Standards. 26 November 2001. Available online: https://www.nist.gov/publications/advanced-encryption-standard-aes (accessed on 25 May 2022). [CrossRef]
2. Tuchman, W. A brief history of the data encryption standard. In *Internet Besieged: Countering Cyberspace Scofflaws*; ACM Press/Addison-Wesley Publishing Co.: New York, NY, USA, 1997; pp. 275–280.
3. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
4. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image. Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
5. Gao, Z.; Chen, D.; Zhang, W.; Cai, S. Colour image encryption algorithm using one-time key and FrFT. *IET Image Process.* **2018**, *12*, 472–478. [CrossRef]
6. Wang, X.; Wang, S.; Zhang, Y.; Luo, C. A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems. *Opt. Lasers Eng.* **2018**, *103*, 1–8. [CrossRef]
7. Hua, Z.; Zhou, Y.; Pun, C.M.; Chen, C.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **2015**, *297*, 80–94. [CrossRef]
8. Zhu, H.; Zhao, Y.; Song, Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **2019**, *7*, 14081–14098. [CrossRef]
9. Bao, H.; Hua, Z.; Wang, N.; Zhu, L.; Chen, M.; Bao, B. Initials-Boosted Coexisting Chaos in a 2D Sine Map and Its Hardware Implementation. *IEEE Trans. Ind. Inform.* **2020**, *17*, 1132–1140. [CrossRef]
10. Gao, X. A color image encryption algorithm based on an improved Hénon map. *Phys. Scr.* **2021**, *96*, 065203. [CrossRef]
11. Assad, S.E.; Farajallah, M. A New chaos-based image encryption system. *Signal Process. Image Commun.* **2016**, *41*, 144–157. [CrossRef]
12. Li, C.; Luo, G.; Qin, K.; Li, C. An image encryption scheme based on chaotic tent map. *Nonlinear Dyn.* **2017**, *87*, 127–133. [CrossRef]
13. Zhang, X.; Wang, X. Multiple-image encryption algorithm based on mixed image element and chaos. *Comput. Electr. Eng.* **2017**, *62*, 401–413. [CrossRef]
14. Li, C.; Lin, D.; Feng, B.; Lü, J.; Hao, F. Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy. *IEEE Access* **2018**, *6*, 75834–75842. [CrossRef]
15. Zhu, C.; Wang, G.; Sun, K. Improved Cryptanalysis and Enhancements of an Image Encryption Scheme Using Combined 1D Chaotic Maps. *Entropy* **2018**, *20*, 843. [CrossRef] [PubMed]
16. Xiong, Y.; Quan, C.; Tay, C.J. Multiple image encryption scheme based on pixel exchange operation and vector decomposition. *Opt. Lasers Eng.* **2018**, *101*, 113–121. [CrossRef]
17. Mishra, D.C.; Sharma, R.K.; Suman, S.; Prasad, A. Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold Transform. *J. Inf. Secur. Appl.* **2017**, *37*, 65–90. [CrossRef]
18. Chai, X. An image encryption algorithm based on bit level Brownian motion and new chaotic systems. *Multi. Tools Apps.* **2015**, *76*, 1159–1175. [CrossRef]
19. Liu, L.; Miao, S. A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus* **2016**, *5*, 289. [CrossRef]
20. Ye, G.; Huang, X. A secure image encryption algorithm based on chaotic maps and SHA-3. *Secur. Commun. Networks* **2016**, *9*, 2015–2023. [CrossRef]
21. Lian, S. Efficient image or video encryption based on spatiotemporal chaos system. *Chaos Solitons Fractals* **2009**, *40*, 2509–2519. [CrossRef]
22. Ye, G.; Huang, X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing* **2017**, *251*, 45–53. [CrossRef]
23. Ye, G.; Pan, C.; Huang, X.; Zhao, Z.; He, J. A Chaotic Image Encryption Algorithm Based on Information Entropy. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850010. [CrossRef]
24. Solak, E.; Çokal, C.; Yildiz, O.T.; Bíyíkoglu, T. Cryptanalysis of Fridrich's Chaotic Image Encryption. *Int. J. Bifurc. Chaos* **2010**, *20*, 1405–1413. [CrossRef]
25. Hua, Z.; Zhou, Y.; Huang, H. Cosine-transform-based chaotic system for image encryption. *Inf. Sci.* **2019**, *480*, 403–419. [CrossRef]
26. Kumar, C.M.; Vidhya, R.; Brindha, M. An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function. *Appl. Intell.* **2022**, *52*, 2556–2585. [CrossRef]
27. Xiao, S.; Yu, Z.; Deng, Y. Design and Analysis of a Novel Chaos-Based Image Encryption Algorithm via Switch Control Mechanism. *Secur. Commun. Netw.* **2020**, *2020*, 7913061. [CrossRef]
28. Li, Z.; Peng, C.; Tan, W.; Li, L. A Novel Chaos-Based Image Encryption Scheme by Using Randomly DNA Encode and Plaintext Related Permutation. *Appl. Sci.* **2020**, *10*, 7469. [CrossRef]
29. Arif, J.; Khan, M.A.; Ghaleb, B.; Ahmad, J.; Munir, A.; Rashid, U.; Al-Dubai, A. A Novel Chaotic Permutation-Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution. *IEEE Access* **2022**, *10*, 12966–12982. [CrossRef]
30. Rijmen, V.; Daemen, J.; Preneel, B.; Bosselaers, A.; Win, E.D. The Cipher SHARK. In *Fast Software Encryption, Proceedings of the 3rd International Workshop on Fast Software Encryption (FSE '96), Cambridge, UK, 21–23 February 1996*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 99–111.

31. Jakobsen, T.P.; Knudsen, L.R. The Interpolation Attack on Block Ciphers. In *Fast Software Encryption, Proceedings of the 4th International Workshop on Fast Software Encryption (FSE '97), Haifa, Israel, 20–22 January 2017*; Springer: Berlin/Heidelberg, Germany, 1997; pp. 28–40.
32. Alexan, W.; ElBeltagy, M.; Aboshousha, A. RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System. *Symmetry* **2022**, *14*, 443. [CrossRef]
33. Abduljabbar, Z.A.; Abduljaleel, I.Q.; Ma, J.; Sibahee, M.A.; Nyangaresi, V.O.; Honi, D.G.; Abdulsada, A.I.; Jiao, X. Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map. *IEEE Access* **2022**, *10*, 26257–26270. [CrossRef]
34. Al-Mashhadi, H.M.; Abduljaleel, I.Q. Color image encryption using chaotic maps, triangular scrambling, with DNA sequences. In Proceedings of the 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), Sulaymaniyah, Iraq, 26–27 April 2017; pp. 93–98.
35. Wang, X.; Su, Y.; Luo, C.; Nian, F.; Teng, L. Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate. *Multim. Tools Appl.* **2022**, *81*, 13845–13865. [CrossRef]