Computers, Materials & Continua
DOI:10.32604/cmc.2022.021077
Article

Tech Science Press

Atmospheric Convection Model Based Digital Confidentiality Scheme

Noor Munir[1], Majid Khan[1,*], Mohammad Mazyad Hazzazi[2], Amer Aljaedi[3], Sajjad Shaukat Jamal[2] and Iqtadar Hussain[4]

[1]Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan
[2]Department of Mathematics, College of Science, King Khalid University, Abha, 61413, Saudi Arabia
[3]College of Computing and Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
[4]Department of Mathematics, Statistics and Physics, Qatar University, Doha, 2713, Qatar
*Corresponding Author: Majid Khan. Email: mk.cfd1@gmail.com
Received: 22 June 2021; Accepted: 04 August 2021

Abstract: Nonlinear dynamics is a fascinating area that is intensely affecting a wide range of different disciplines of science and technology globally. The combination of different innovative topics of information security and high-speed computing has added new visions into the behavior of complex nonlinear dynamical systems which uncovered amazing results even in the least difficult nonlinear models. The generation of complex actions from a very simple dynamical method has a strong relation with information security. The protection of digital content is one of the inescapable concerns of the digitally advanced world. Today, information plays an important role in everyday life and affects the surroundings rapidly. These digital contents consist of text, images, audio, and videos, respectively. Due to the vast usage of digital images in the number of social and web applications, its security is one of the biggest issues. In this work, we have offered an innovative image encryption technique based on present criteria of confusion and diffusion. The designed scheme comprises two major nonlinear dynamical systems. We have employed discrete fractional chaotic iterative maps to add confusion capability in our suggested algorithm and continuous chaotic Lorenz system. We have verified our offered scheme by using statistical analysis. The investigations under the statistical tests suggested that our proposed technique is quite reasonable for the security of digital data.

Keywords: Lorenz atmospheric convection model; fractional logistic map; image encryption; S-box

1 Introduction

Nowadays, society is full of the sphere of information in a different form of the digital medium. The advancement in different private and public sectors demands new and innovative results towards handling big data with low-cost technologies. Digital information that travels through an insecure line of communication plays an important role because of emerging technology usage at a high scale on

social media and web applications etc. This insecurity while utilizing these applications on small and large computational machines lost the confidence of the net user. The issue of information security not just stops here it extended towards the regime of corporate organizations which includes business, banking sectors, and commercial firms. The information breaches are now increasing widely due to the vast number of facilities available online for instance transactions and online banking. The online services increased by a daily boom of commercial organizations due to competition among different officialdoms in an advanced era. Different companies created their research and development teams that mainly deal with cybersecurity. The security of information and online data streams gradually increase to fifth-generation technologies and the same happened in the area of information security where one cannot remain away from cybersecurity attacks. There have been several mechanisms used for the security of information which includes cryptography, watermarking, and steganography. The privacy of the given information can be assured by using cryptography. The watermarking and information hiding techniques are utilized for both information integrity and authentication. The most fruitful area of information preserving, and confidentiality is chaotic cryptography. With the advancement in the area of nonlinear dynamics, several discrete and continuous chaotic systems were developed and tested against different chaotic tests. The relations between chaos and cryptography have been a mode of discussion for two decades [1]. Similarities among different concepts of chaos and cryptography make it a reasonable candidate for the encryption of digital data. The notion of diffusion and confusion in 1949 proposed by Claude Shannon added new directions in information security. Then different new block ciphers were designed which used confusion and diffusion. The addition of diffusion and confusion in a block cipher added a robust security layer against different cryptographic attacks. In modern cryptosystems, the notion of Claude Shannon is term as substitution-permutation network (SP-network) [2]. The idea of confusion is to make the relations between encrypted data and secret key as difficult as possible which can be achieved through substitution, whereas diffusion is used to scatter the statistical construction of original information over the greater part of encrypted information [3]. The diffusion is achieved through permutation which simply means to reorder certain bits. By utilizing SP-network collectively, it is quite hard to detect any non-uniform change in cipher-text. The same idea of SP-network is now followed by different chaos-based encryption algorithms [4–11].

Several image encryption schemes utilized chaotic dynamical systems for the confidentiality of digital contents [12–16]. Chaotic schemes were also helpful for the formulation of nonlinear components of block cipher known as Substitution boxes (S-boxes) [17–21]. The principal idea of constructing nonlinear components through chaotic dynamical systems is to add strong confusion capability which is surely one of the vital components in modern block ciphers. There exist many encryption structures in literature with weak security and vulnerability in implementation design due to skipping the notion of confusion and diffusion [22–25]. A small change in chaotic parameters produces a dynamically different trajectory similarly small variations in chaotic parameters produce a completely new substitution box. The main contribution of this work is as follows:

1. The idea of this research is to produce a nonlinear component by using a fractional chaotic logistic map.
2. Implementation of constructed S-box in the suggested chaos-based image encryption method.
3. The scheme also entails a continuous chaotic Lorenz system for diffusion that ultimately produces permutation [6].
4. Some security assessments are performed to examine the efficiency and robustness of offered system along with some statistical analysis.

This manuscript consists of seven sections. The basic concepts are reviewed in Section 2. The mathematical model of the Lorenz chaotic system is offered in Section 3. The offered substitution box and image encryption technique are presented in segments 4 and 5 correspondingly. The statistical analyses are presented in Section 6. As a final point, the conclusion is shown in the last section.

2 Backgrounds

In this section, we have presented some basic keys, which are essential for the interpretation of innovative image encryption techniques though suggested S-box based on discrete fractional chaotic iterative maps.

2.1 Logistic Map

The logistic map is one of the prominent and extensively utilized one dimensional (1-D) discrete logistic chaotic map proposed by R. M May, whose state evolves corresponding to the following mathematical equation [4]:

$$y_{n+1} = \mu y_n(1 - y_n), \tag{1}$$

where $0 \leq \mu \leq 4$ represent the control parameter and logistic map with state variable y_n whose behaviors depend on the initial condition y_0. The chaotic outputs y_n of the map defined in Eq. (1) are bounded within the interval $[0,\ 1]$ for all $n \geq 0$.

2.2 Riemann-Liouville Fractional Derivative

If $f(y) \in C([a, b])$ and $a < x < b$ then [5]:

$$I^{\alpha}_{a+}f(y) = \frac{1}{\Gamma(\alpha)}\int_0^{\alpha}\frac{f(t)}{(x-t)^{t-\alpha}}dt, \tag{2}$$

where α ranges from $-\infty$ to ∞ and known as the Riemann-Liouville fractional integral having order α. In the same way for $\alpha \in]0, \infty[$ we let

$$D^0_{a+}f(y) = I^0_{\alpha}f(y) = f(y), \tag{3}$$

is known as Riemann-Liouville fractional derivative with order α [6].

2.3 Fractional Logistic Equation

For all $y \geq 0$, $\lambda > 0$ and $\alpha \in]-\infty, \infty[$:

$$Q_{\lambda}{}^{\alpha}(y) = \frac{\lambda}{\Gamma(\alpha+2)}\left(1 - \frac{2x}{\alpha+2}\right)y^{1+\alpha}, \tag{4}$$

which is called fractional logistic equation (FLE) of order α.

3 Mathematical Formulation of Atmospheric Convection Model

In 1963, Edward Lorenz proposed a simple mathematical model for atmospheric convection. The mathematical derivation of Lorenz equations is given in [6,7]. There are three different models of chaotic Lorenz systems which are given as follows:

Viscosity + diffusion:

$$\begin{aligned} \dot{x} &= -\sigma x, \\ \dot{y} &= -xz - y + \gamma x, \\ \dot{z} &= xy - \beta z. \end{aligned} \tag{5}$$

Buoyancy + diffusion:

$$\begin{aligned} \dot{x} &= -\sigma y, \\ \dot{y} &= -xz - y + \gamma x, \\ \dot{z} &= xy - \beta z. \end{aligned} \tag{6}$$

Viscosity + buoyancy

$$\begin{aligned} \dot{x} &= -\sigma x + \sigma y, \\ \dot{y} &= -xz, \\ \dot{z} &= xy. \end{aligned} \tag{7}$$

4 Proposed S-Box Using Fractional Chaotic Map

The one-dimensional logistic map which was designed in 1967 by May [4] is one of the modest discrete nonlinear chaotic schemes which shows chaotic performance; its mathematical equation is described by the following iterative formula.

$$y_{n+1} = Q_\lambda(y) = \lambda y(1 - y). \tag{8}$$

By using the concept of the fractional logistic map, taking $\alpha = 0$ and considering the fractional powers we purpose a chaotic fractional equation as

$$y_{n+1} = Q_\lambda(y_n) = \lambda y_n^g (1 - y_n^h), \tag{9}$$

where x is variable of the map and x_0 decide the initial state, λ is a system parameter, g and h are positive fractional powers and n represents the number of iterations desired to be applied. The initial value λ and x_0 acts as a private key when utilized in the encryption structure. To effectively decrypt the data, accurate values of both λ and x_0 are required at the receiver's end. Therefore, the system turns out to be completely key-dependent which creates the retravel of secret data from the encrypted information complicated for the assailant. By using this fractional logistic map and the assumptions $g = 1.5,\ h = 1.5$ and $\lambda = 3.5$ we purposed 16×16 S-box over $GF(2^8)$ (see Tab. 1).

Table 1: Proposed S-box by using chaotic fractional equation

D8	09	F8	29	56	26	98	C9	D9	C8	79	68	99	88	39	28
5C	85	7C	A5	BC	E5	1C	45	55	4C	F5	EC	15	0C	B5	AC
54	8D	74	AD	B4	ED	14	4D	5D	44	FD	E4	1D	04	BD	A4
BF	22	DF	42	1F	82	7F	E2	F2	AF	92	4F	B2	6F	52	0F
12	CF	32	EF	72	2F	D2	8F	9F	02	3F	A2	5F	C2	E1	62
1A	C7	35	E7	7A	27	DA	87	97	0A	37	AA	57	CA	F7	6A
96	4B	B6	6B	F6	AB	56	0B	1B	86	BB	26	DB	46	7B	E6
9E	43	BE	63	FE	A3	5E	03	13	8E	B3	2E	D3	4E	73	EE

(Continued)

Table 1: Continued

33	AE	53	CE	93	0E	F3	6E	7E	23	1E	C3	3E	E3	DE	83
3B	A6	5B	C6	9B	06	FB	66	76	2B	16	CB	36	EB	D6	8B
75	6C	95	8C	D5	CC	35	2C	3C	65	DC	05	FC	25	9C	C5
E0	01	00	21	40	61	A0	C1	D1	D0	71	70	91	90	31	30
F1	F0	11	10	51	50	B1	B0	C0	E1	60	81	80	A1	20	41
F9	E8	19	08	59	48	B9	A8	B8	E9	58	89	78	A9	18	49
B7	2A	D7	4A	17	8A	77	EA	FA	A7	9A	47	BA	67	5A	07
7D	64	9D	84	DD	C4	3D	36	52	6D	D4	0D	F4	2D	94	CD

5 Suggested Image Encryption Algorithm

In this segment, a fractional chaotic S-box-based image encryption technique is suggested. The intended scheme offers less computational time and cost of image encryption parallel to other methods which are available in the literature. The working steps of offered encryption scheme are as follows:

Step 1: Choose a standard color image as input having size $n \times m$.

Step 2: Divide the digital color image into three channels that are Red, Green, and Blue.

Step 3: Utilize different proposed substitution boxes on each image layer individually.

Step 4: Run Lorenz fractional chaotic equations and store all the generated output in one matrix.

Step 5: Arrange matrix in ascending order by using the command of the sort in MATLAB and store the sorting position of each element in one matrix.

Step 6: Now shuffle the pixels of each image layer corresponding to the sorting position matrix obtained in step 5.

Step 7: Apply bitwise XOR with random array generated from Lorenz chaotic equation on each layer of the image obtained in step 6.

Step 8: Concatenate all the layers produced from step 7 in one image.

Step 9: The image attained from step 8 is the required encrypted image.

The structure diagram of the offered image encryption algorithm is depicted in Fig. 1.

Decryption of Image

The procedure of decryption is the same as the encryption procedure in reverse order. The original image can be retrieved easily by utilizing the decryption procedure. Figs. 2 and 3 show some standard layer-wise encrypted images through the proposed scheme.

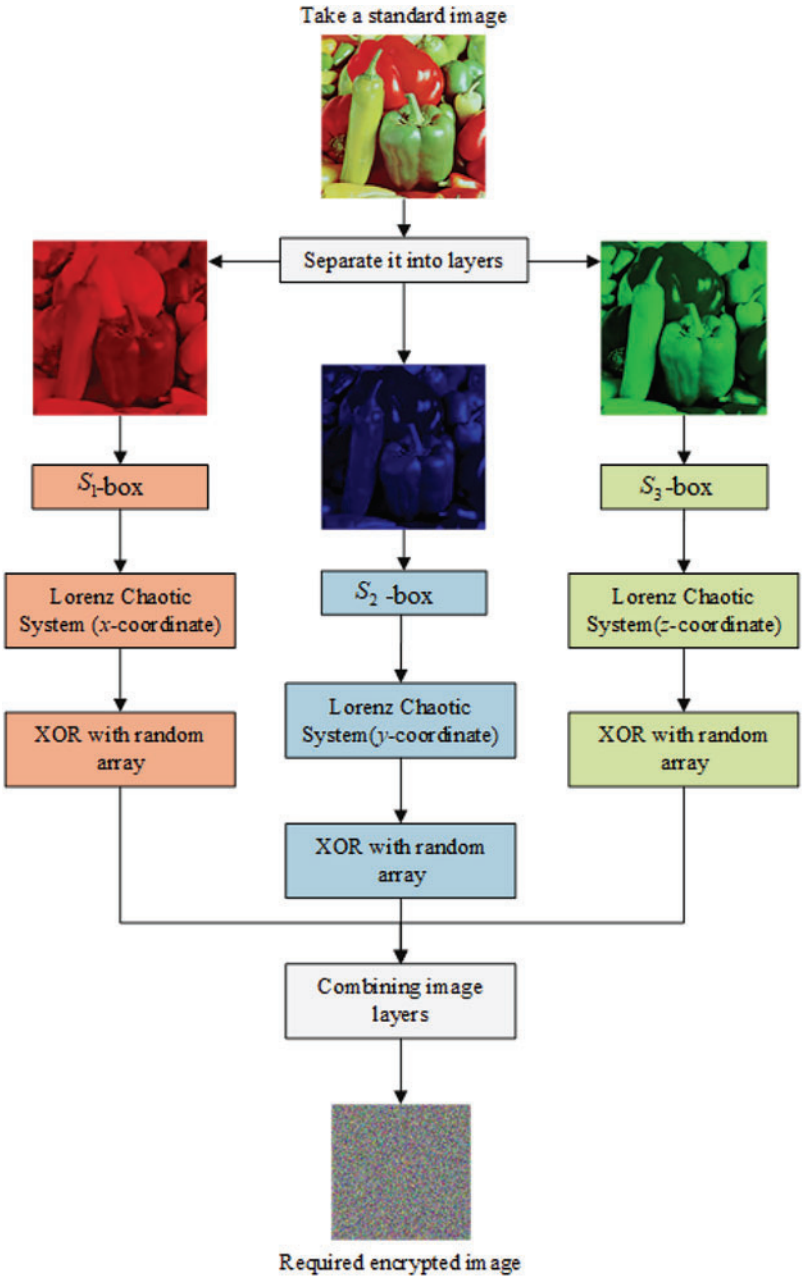

Figure 1: Design of proposed encryption scheme

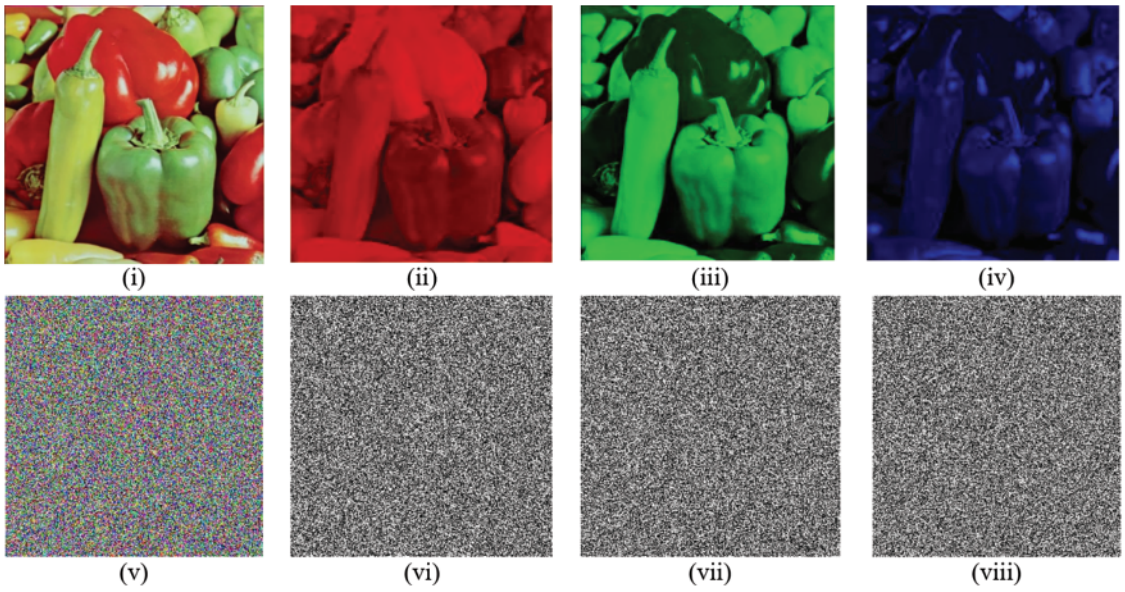

Figure 2: (i–iv) Original layers of peppers image (v–viii) Encrypted layers of Peppers image

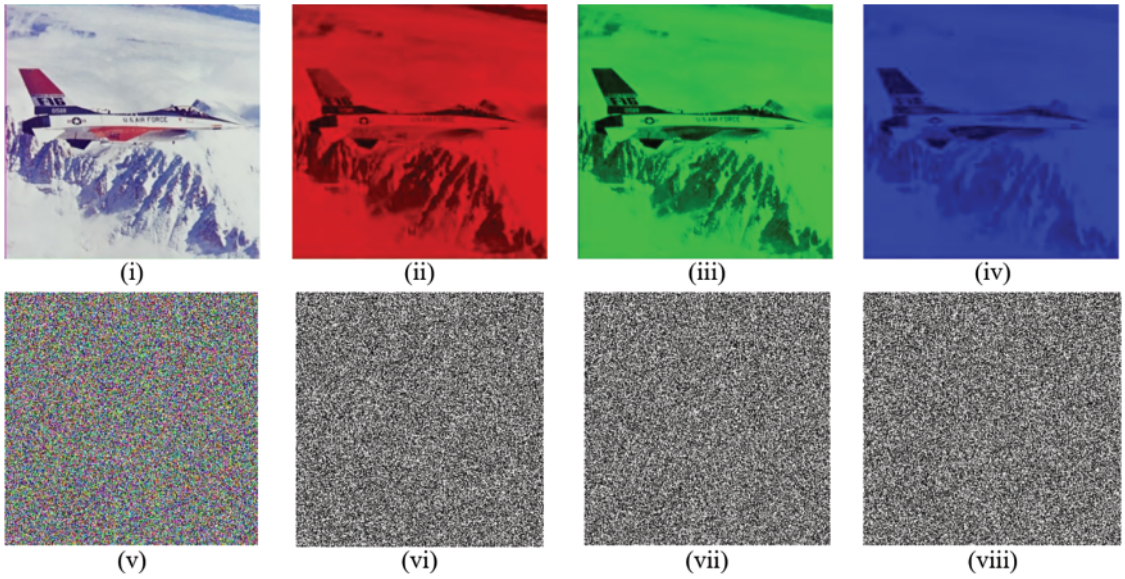

Figure 3: (i–iv) Original layers of airplane image (v–viii) Encrypted layers of Airplane image

6 Security Assessment of Suggested Technique

This part of the manuscript describes various safety constraints to explain the robustness of the suggested technique. Some statistical analyses are accumulated by utilizing plain and their respective cipher images. These statistical analyses comprise correlation, entropy, uniformity, similarity measures, pixel modification, and sensitivity of plaintext. Each of the analyses is examined in an aspect to validate the efficiency of the encryption technique [15,16].

6.1 NIST Analysis

The randomness of a cipher can also be determined by NIST-800-22 test suite offered by the National Institute of Standard and Technology in 2001. NIST suite comprises several tests to analyze the arbitrariness in output data with probability values (p values). The p-values of each assessment must be greater than 0.001 for a robust encryption scheme. The results of NIST for Peppers encrypted image of size 256×256 are depicted in Tab. 2. The obtained results reflect that the encrypted image layers are highly randomized therefore, the offered encryption scheme is robust against all statistical attacks.

Table 2: NIST test results for Peppers cipher image

Test Name		p values for enciphered image		
		Red	Green	Blue
Frequency		0.34278	0.046345	0.1641
Block-frequency		0.95341	0.22203	0.083407
Runs (M = 10,000)		0.9131	0.527	0.37624
Long runs of ones		0.035752	0.035752	0.03572
Rank		0.29191	0.29191	0.29191
Spectral DFT		0.30979	0.66336	0.56166
No overlapping templates		1	0.9994	0.9994
Overlapping templates		0.85988	0.85988	0.85988
Universal		0.98754	0.998549	0.9927
Serial	*p values 1*	0.8456	0.000538	0.045993
Serial	*p values 2*	0.95358	0.014294	0.14871
Approximate entropy		0.94449	0.10512	0.18385
Cumulative sums forward		0.24091	0.11794	0.20017
Cumulative sums reverse		0.77506	1.8019	0.39016
Random excursions	$X = -2$	0.84634	0.79201	0.45423
	$X = -1$	0.11873	0.7127	0.78329
	$X = 1$	0.23666	0.87691	0.90414
	$X = 2$	0.68967	0.5962	0.26123
Random excursions variants	$X = -2$	0.34278	0.083265	0.61112
	$X = -1$	0.85513	0.024449	0.52184
	$X = 1$	0.715	0.2113	0.33667
	$X = 2$	0.75183	0.5637	0.16552

6.2 Histogram Analysis

The histogram is the plot of the number of pixels for each tonal value. The histogram of original images contains sharp peaks in its distribution. An ideal encryption scheme yields a cipher image with uniform histogram distribution. 3D histograms of the plain and enciphered Peppers image of size 256×256 image layers are displayed in Fig. 4. From experiments, we can analyze that the scattering of pixels of the encrypted images is uniform, which can extensively decrease the values of correlation among the pixels. Consequently, histogram analysis indicates that our encryption algorithm is protected besides attacks.

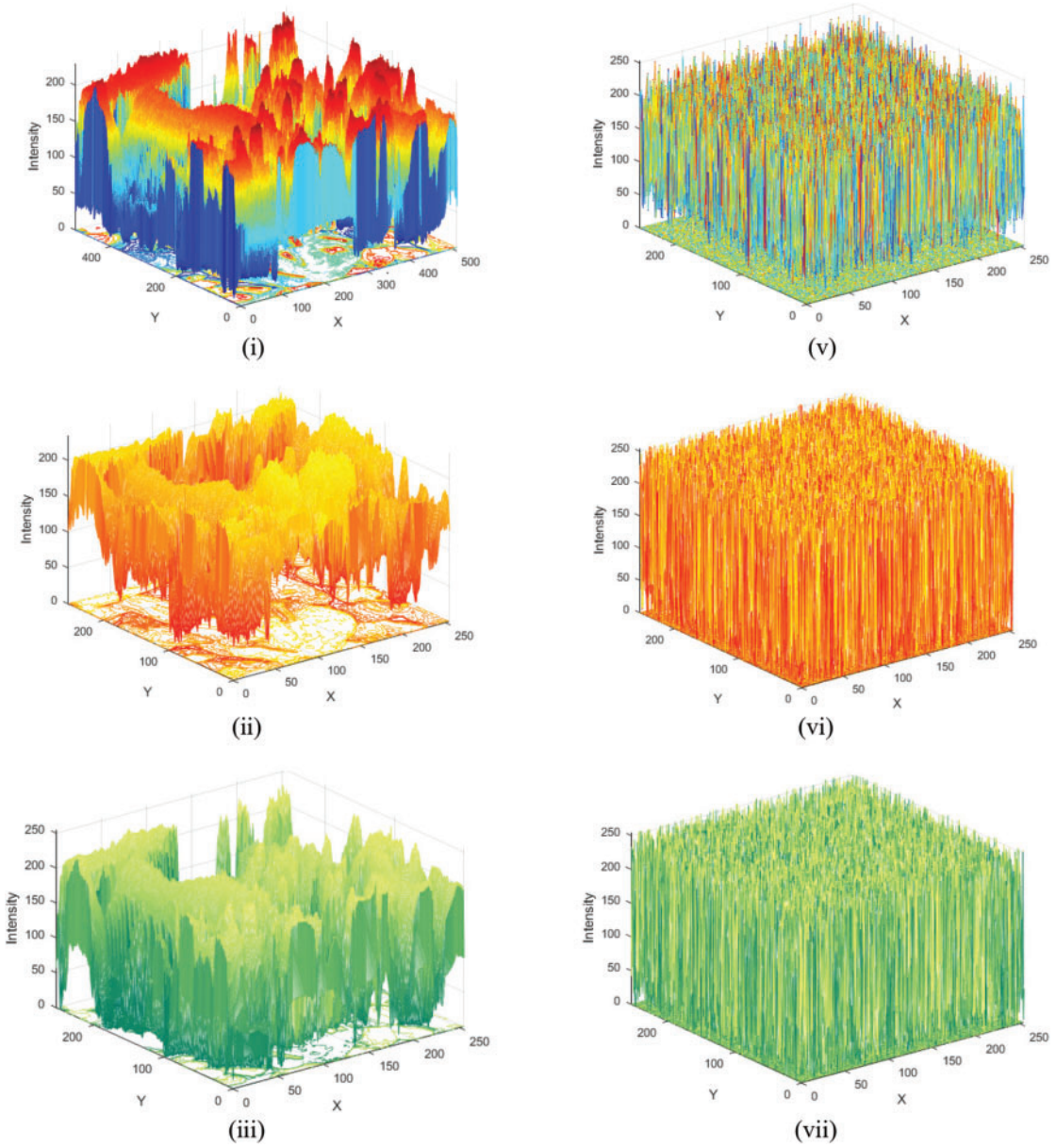

Figure 4: Continued

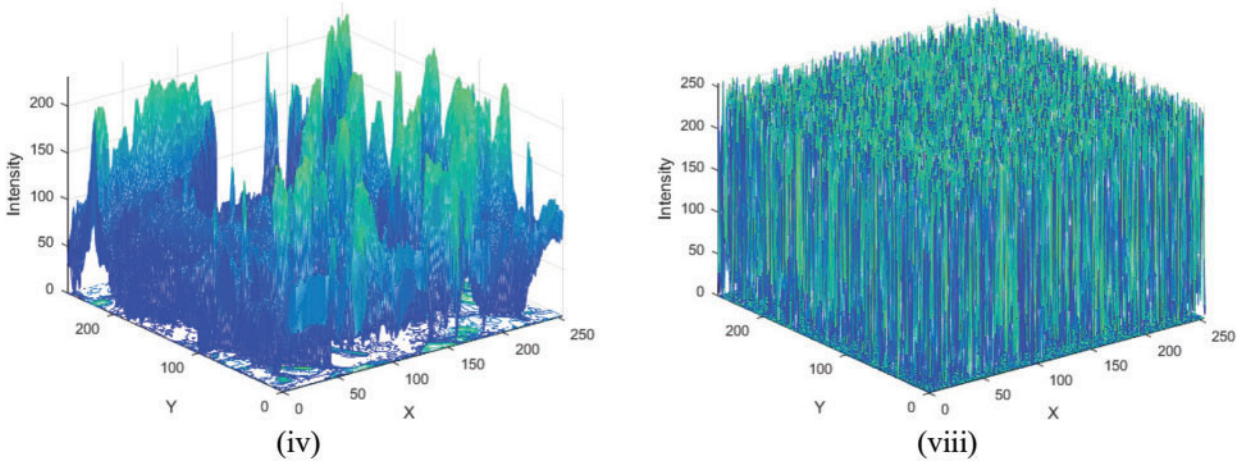

Figure 4: (i–iv) Histograms of peppers image of size 256 × 256 original layers (v–viii) Histograms of peppers image encrypted layers

6.3 Correlation Analysis

The neighboring pixels of an image are highly correlated in horizontal, diagonal, and vertical directions. The original image exhibits the high correlation value, and alternatively, for an ideal encryption scheme, the correlation value must be less and approximately near to 0. A smaller value of the correlation of encrypted images leads to a secure encryption algorithm which reduces the possibility of attacks. The correlation coefficient of image pixels can be calculated by:

$$C_{M,N} = \frac{\sum_{i}^{n} (M_i - \bar{M})(N_i - \bar{N})}{||(M_i - \bar{M})||||(N_i - \bar{N})||}, \tag{10}$$

where

$$||(M_i - \bar{M})|| = \sqrt{\sum_{i=1}^{n} (M_i - \bar{M})^2} \text{ and } ||(N_i - \bar{N})|| = \sqrt{\sum_{i=1}^{n} (N_i - \bar{N})^2}, \tag{11}$$

where M and N are the estimations between two nearby pixels at grayscale in the digital image. The correlation coefficients for the plain and enciphered image along horizontal, vertical, and diagonal axes are presented in Tab. 3.

Table 3: Color components wise correlation coefficient of plain and enciphered images

Image		Original image				Cipher image			
		Gray	R	G	B	Gray	R	G	B
Pepper	H	0.9635	0.9647	0.9719	0.9578	−0.0057	−0.0059	−0.0023	−0.0048
	V	0.9707	0.9683	0.9776	0.9665	−0.0128	−0.0093	−0.0003	−0.0149
	D	0.9363	0.9364	0.9505	0.9287	−0.0027	−0.0048	−0.0001	−0.0028

(Continued)

Table 3: Continued

Image		Original image				Cipher image			
		Gray	R	G	B	Gray	R	G	B
	H	0.8730	0.9394	0.8828	0.9251	−0.0049	−0.0086	−0.0007	−0.0110
Baboon	V	0.8323	0.9166	0.8542	0.9163	−0.0178	−0.0068	−0.0121	−0.0024
	D	0.7889	0.8968	0.8102	0.8806	−0.0002	−0.0064	0.0036	−0.0064
	H	0.9352	0.9353	0.9364	0.9342	−0.0122	−0.0024	−0.0091	−0.0083
Airplane	V	0.9296	0.9244	0.9361	0.9010	−0.0203	−0.0041	−0.0123	−0.0031
	D	0.8795	0.8721	0.8864	0.8613	0.0009	−0.0054	0.0053	0.0005
	H	0.9178	0.9166	0.9435	0.9265	−0.0103	−0.0022	−0.0012	−0.0044
House	V	0.9337	0.9234	0.9298	0.9321	−0.0135	0.0071	−0.0098	−0.0087
	D	0.8665	0.8238	0.8565	0.8873	−0.0019	0.0056	−0.0019	0.0005
	H	0.9007	0.9095	0.9376	0.9469	−0.0031	0.0076	−0.0010	−0.0084
Jellybeans	V	0.9132	0.9187	0.9129	0.9668	−0.0034	0.0017	−0.0089	−0.0024
	D	0.9117	0.9234	0.9645	0.8998	−0.0013	0.0065	−0.0091	0.0015
	H	0.9112	0.9342	0.9476	0.9945	−0.0018	−0.0049	0.0027	0.0014
Sailboat	V	0.9256	0.9232	0.9277	0.9545	−0.0011	0.0036	−0.0048	0.0016
	D	0.9721	0.8154	0.8843	0.9853	−0.0091	0.0038	0.0024	0.0045
	H	0.8991	0.8982	0.9165	0.9267	−0.0072	0.0084	−0.0067	−0.0061
Splash	V	0.8814	0.9144	0.9188	0.9354	−0.0037	0.0106	−0.0015	−0.0102
	D	0.9018	0.9643	0.8992	0.8994	−0.0114	0.0054	−0.0039	0.0018
	H	0.9700	0.9611	0.9735	0.9686	−0.0146	0.0000	−0.0084	−0.0060
Tree	V	0.9475	0.9345	0.9536	0.9450	−0.0208	−0.0081	−0.0115	−0.0067
	D	0.9309	0.9131	0.9390	0.9282	0.0070	0.0017	0.0028	0.0028

where H, V, and D shows the horizontal, vertical, and diagonal direction of the image, respectively. To quantify the correlation coefficient, we randomly choose 2500 sets of two adjoining pixels in three ways (horizontal, diagonal, and vertical) from encrypted and original image data. Tab. 3 presents the corresponding experimental results. From Tab. 3 we can examine that the values of correlation of original images are near to one, whereas the values of correlation of the enciphered images are near to 0. From the depicted results we can see that the suggested encryption technique reduces the correlation among image pixels accurately. Fig. 5, presents the adjacent pixel distributions in the horizontal, diagonal, and vertical axes for Peppers images. Figs. 5i–5iv presents the correlation of plain images, although Figs. 5v–5viii represents the correlation of encrypted images. As from these Fig. 5, we can see that the plain images exhibit high values of correlation, on the other hand, the enciphered images have a random distribution of correlation. The test results indicate that our encryption scheme has a very good influence on decreasing correlation. Therefore, the offered encryption algorithm is robust against all the attacks related to the correlation of pixels.

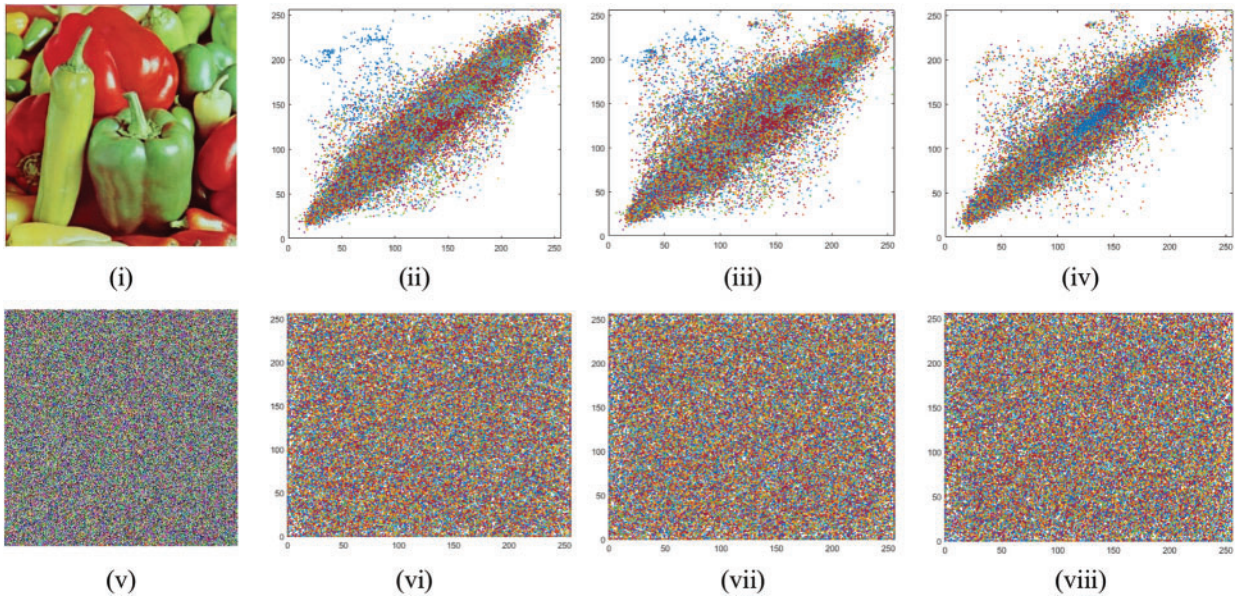

Figure 5: (i–iv) Correlation coefficient among pixel pairs for plain peppers image; (v–viii) Correlation coefficient among pixel pairs for enciphered peppers image

6.4 Information Entropy

The distribution of gray values of the image is evaluated as the information entropy. Entropy increases with an increase in the uniformity of distribution of gray values. The encryption scheme is said to be highly secure if less information is leaked from the gray distribution value of images. Information entropy can be measured by the mathematical equation:

$$H = -\sum_{i=0}^{2^N-1} p_i \log_2 p_i, \tag{12}$$

where p_i shows the gray value probability. The perfect value of encrypted image entropy is 8. The entropy of the enciphered image for the standard Lena image produced by the suggested scheme is 7.9991. The entropy of the enciphered image for Peppers image enumerated by the suggested scheme is 7.9990 and for Airplane image information entropy is 7.9991. These values are very near to the absolute value of entropy. Entropies of numerous original and enciphered images are analyzed which are listed in Tab. 4. These values of entropy regard that they are very near to the perfect value 8. This shows that the encryption technique is safe against all feasible assaults.

Table 4: Plain and encrypted images information entropies

Images	Original image	Layers of plain image			Enciphered image	Layers of enciphered image		
		R	G	B		R	G	B
Pepper	7.7253	7.3090	7.6004	7.1353	7.9990	7.9975	7.9971	7.9971
Baboon	7.7666	7.6192	7.3637	7.6437	7.9991	7.9970	7.9976	7.9973
Airplane	6.6879	6.7421	6.8249	6.2475	7.9991	7.9974	7.9972	7.9973
House	7.5112	7.4187	7.2486	7.4586	7.9990	7.9971	7.9972	7.9973
Jellybeans	6.6098	5.3111	5.7424	6.5942	7.9991	7.9972	7.9973	7.9972
Sailboat	7.7675	7.2688	7.6146	7.2471	7.9989	7.9971	7.9973	7.9968
Splash	7.3232	7.0303	6.9567	6.1310	7.9991	7.9970	7.9973	7.9972
Tree	7.5634	7.2798	7.4610	6.9923	7.9991	7.9975	7.9975	7.9971

6.5 Distance Based Measurements

The image quality assessment based on pixel modification measures are done by calculating maximum difference (MD), mean square error (MSE), the average difference (AD), peak signal to noise ratio (PSNR), normalized correlation (NCC), normalized absolute error (NAE) and structure content value (SC). These are the error metrics that are utilized to compare different images.

Maximum Difference is also known as MD shows the maximum difference among the plain and enciphered images. The maximum difference can be represented in the mathematical form as follows:

$$MD = \max(|O_{xy} - E_{xy}|), \quad x = 1, 2, \ldots, n, \quad y = 1, 2, \ldots, m. \tag{13}$$

Our analyzed results are presented in Tab. 5 which reflects that with the boost in the value of MD, the robustness of the encryption structure is increased.

The normalized absolute error also named NAE is represented in mathematical form as follows:

$$NAE = \frac{\sum_{x=1}^{X}\sum_{y=1}^{Y}|O_{xy} - E_{xy}|}{\sum_{x=1}^{X}\sum_{y=1}^{Y}|E_{xy}|}, \tag{14}$$

NAE defines the proportion of how far the enciphered digital data is from the plain image with the estimation of zero being impeccable similar images. From Tab. 5, we can see that the increase in the approximation of normalized absolute error demonstrates a good description of scrambled images with encryption procedure.

The average difference can be mathematically defined as:

$$AD = \frac{1}{X \times Y}\sum_{x=1}^{X}\sum_{y=1}^{Y}(O_{xy} - E_{xy}). \tag{15}$$

Table 5: Correlation-based and pixel difference-based measures of suggested encryption technique

Image	Quality evaluation measures			Pixel difference measures			Similarity measures		
	MAE	MSE	PSNR	NAE	AD	MD	SSIM	SC	NCC
Pepper	84.64	5393.27	10.81	0.4951	−7.5098	216	0.0214	0.9168	0.8895
Airplane	75.88	7302.30	9.49	0.3987	51.8224	221	0.0216	1.8231	0.6675
Baboon	74.65	4087.22	12.01	0.4239	−5.6385	199	0.0205	0.8694	0.9505
House	64.78	5888.67	10.43	0.3892	34.2937	232	0.0187	1.5084	0.7273
Jellybeans	78.11	6342.48	10.10	0.3777	48.6930	201	0.0229	1.7347	0.6904
Sailboat	68.37	6757.83	9.83	0.5436	−2.0939	219	0.0207	1.0596	0.8020
Splash	81.49	5747.85	10.53	0.5935	−24.0886	246	0.0210	0.7086	0.9893
Tree	61.63	7098.94	9.61	0.5419	2.0179	224	0.0161	1.1339	0.7739

The value of the average difference is preferably zero for two similar digital images. The calculated results of the average difference are presented in Tab. 5, which indicates that the suggested technique is robust against all possible differential assaults.

6.6 Mean Squared Error and Peak Signal to Noise Ratio Analysis

The encryption technique utilized to the original data adds noise to the actual digital contents therefore an encrypted digital image is not equivalent to the plain digital image. We process the MSE among the plain and encrypted images to evaluate the level of encryption. MSE can be formulated in mathematical form as:

$$MSE = \frac{\sum_{x=1}^{X}\sum_{y=1}^{Y}(O_{xy} - E_{xy})^2}{X \times Y}, \tag{16}$$

where O_{xy} and E_{xy} allude to pixels situated at x^{th} row and y^{th} column of the plain and encrypted image individually. Higher the MSE value, increase the robustness of encryption. The enciphered image quality is evaluated using peak signal to noise ratio (PSNR), which is represented by the mathematical formula:

$$\text{PSNR} = 20\log_{10}\left[\frac{I_{MAX}}{\sqrt{MSE}}\right], \tag{17}$$

where I_{MAX} is the highest pixel approximation of the image. The PSNR ought to be minimal value when equates to the enormous difference among original and encrypted images. Results in Tab. 5 clearly show that the suggested technique is very near to the ideal values of MSE and PSNR, therefore the scheme is secure against security threats.

6.7 Similarities Measures

Normalized cross-correlation, structure content, and structure similarity are utilized to estimate the resemblances between two signals. These are some standard analyses for measuring that original and encrypted images are analogous or different.

Normalized cross-correlation also known as NCC has been generally utilized as a metric. To check the level of difference (or resemblance) between two images. The NCC ranges from –1 and 1. Mathematically, the normalized correlation of the image is computed by the given formula [16–21]:

$$NCC = \frac{\sum_{x=1}^{X}\sum_{y=1}^{Y} O_{xy} \times E_{xy}}{\sum_{y=1}^{Y} E_{xy}{}^{2}}, \tag{18}$$

where $X \times Y$ denotes the size of plain image O and cipher image E both. Our analyzed results presented in Tab. 5 reveals that the calculation of NCC for encryption is near to unity which distinctly means that the suggested technique contains strong divergences among the pixels of original and enciphered images.

Structural content is also known as SC, measures the collective weight of a plain image to the respective encrypted image. It is, hence, a global metric. If the value of SC exhibits as one, at that point the encrypted image represents the better quality, and an increase in the assessment of SC denotes that the image is very low in quality. The mathematical form of structural content is as:

$$SC = \frac{\sum_{x=1}^{X}\sum_{y=1}^{Y}(O(y,k))^2}{\sum_{x=1}^{X}\sum_{y=1}^{Y}(E(y,k))^2} \tag{19}$$

From Tab. 5 we can observe that our encryption technique gives the evaluation of SC which is not very near to unity due to the diffusion and confusion like noise disorder in the plain image.

6.8 Plaintext Sensitivity Analysis

To check the randomness of the encryption technique, diffusion is an important constraint that must be assessed. Two basic methods are implemented recognized as the number of changing pixel rate (NPCR), and the unified averaged changed intensity (UACI) to examine the impact of one-bit alteration in the plain content and the enciphered content. NPCR focuses on the number of pixels that change the assessment in differential assaults although the UACI concentrates on the AD (averaged difference) among two paired enciphered images. Assume encrypted image previously and afterward, one-pixel change in original content image is C_1 and C_2 correspondingly. The value of pixels at grid (x, y) in E_1 and E_2 are symbolized as $E_1(x, y)$ and $E_2(x, y)$, D a bipolar array is described by Eq. (20). Formerly the MAE, UACI, and NPCR can be formulated by the subsequent representations:

$$\text{NPCR} = \frac{\sum_{x,y} D(x,y)}{W \times H} \times 100\%, \tag{20}$$

where

$$D(x,y) = \begin{cases} 0, & E_1(x,y) = E_2(x,y) \\ 1, & E_1(x,y) \neq E_2(x,y), \end{cases} \tag{21}$$

$$UACI = \frac{1}{W \times H} \sum_{x=0}^{X-1} \sum_{y=0}^{Y-1} \left| \frac{E_1(x,y) - E_2(x,y)}{255} \right| \times 100\%, \tag{22}$$

Tab. 6 presents the values of, UACI (≈33%) and NPCR (>99%) for every layer of image for nine different standard images. Investigational consequences demonstrate the estimated variance of UACI and NPCR are actual near to the theoretical measures, which explain the validity of theoretical standards. Hence our proposed encryption method is resilient against differential attacks.

Table 6: The results of sensitivity analysis of suggested encryption technique

Image	Differential analysis		NPCR			UACI		
	NPCR	UACI	R	G	B	R	G	B
Pepper	99.982	33.27	99.675	99.991	99.976	33.09	33.38	33.32
Airplane	99.995	33.22	99.883	99.994	99.987	33.48	33.27	33.16
Baboon	99.994	33.33	99.643	99.835	99.911	33.58	33.47	33.22
House	99.893	33.18	99.763	99.758	99.967	33.27	33.12	33.08
Jellybeans	99.981	33.08	99.897	99.879	99.990	33.06	32.98	33.36
Sailboat	99.989	33.29	99.954	99.952	99.985	33.34	33.03	33.27
Splash	99.972	33.01	99.814	99.889	99.988	33.36	32.82	32.91
Tree	99.989	33.15	99.994	99.976	99.937	33.07	33.25	32.98

6.9 Z_1 Test for Randomness (0–1 Test)

In this section, we have applied the 0–1 test for the chaos which checks the randomness of enciphered images. When the value of the Z1 test is near to one it means that the proposed scheme defines good randomness which shows that it is secure against differential attacks. On the other side, if the value of this test is near zero, this means the test is failed and there is no chaos in the encrypted image. Here we have presented analyzed results in Tab. 7 which defines the Z1 test value for the layer-wise encrypted image.

6.10 Comparative Analysis with Standard Results

In this section, we compare the suggested encryption method with numerous states of the arts, which have high security. The comparison contains the following aspects: information entropy, correlation among different pixels of encrypted images, robustness to plaintext sensitivity analysis. Furthermore, from our experimental results, we can see that correlation values are high between three R, G, and B layers for plain color digital images, which makes data revelation conceivable. Moreover, we have presented a contrast of correlation coefficient of Pepper 256 × 256 image enciphered with our suggested technique and some encryption method already described in the literature (see Tab. 8).

Here we have offered a contrast of values of entropy of Pepper 256 × 256 image encrypted with our proposed scheme and some encryption method already described in the literature (see

Table 7: Z_1-Test for of enciphered image

Image	Z_1-Test values			Test result
	R	G	B	
Pepper	0.9986	0.9955	0.9967	Qualify
Baboon	0.9967	0.9964	0.9974	Qualify
Airplane	0.9976	0.9986	0.9974	Qualify
Fruits	0.9975	0.9979	0.9972	Qualify

Table 8: Contrast of the correlation of suggested technique with current procedures using Pepper image

S. no	Method	Direction	Correlation value
1.	Proposed Scheme	Horizontal	−0.0057
		Vertical	−0.0128
		Diagonal	−0.0027
2.	Liu et al. [10]	Horizontal	−0.0351
		Vertical	−0.0028
		Diagonal	0.0475
3.	Liu et al. [12]	Horizontal	0.0009
		Vertical	0.0009
		Diagonal	−0.0015

Tab. 9). Subsequently, the suggested image encryption technique is robust adjacent to the entropy attack. Moreover, the entropy assessments of the suggested method are better as contrasted to other encryption schemes. The entropy of the recommended technique for encrypted Pepper image is improved than current methods by inspecting Tab. 9.

Table 9: Comparative analysis for the entropy of Pepper image of size 256×256

S. no	Technique	Entropy
1	Offered technique	7.9990
2	Liu et al. [10]	7.9878
3	Abd El-Latif et al. [11]	7.9990
4	Liu et al. [12]	7.9895

Thus, we have presented a UACI and NPCR of Pepper 256 × 256 image enciphered with our suggested technique with some other encryption methods to show the better performance of the suggested scheme in Tab. 10. From depicted results, we can see that our offered scheme is more resilient as compared to other techniques.

Table 10: Contrast of differential attacks analysis

S. no	Technique	UACI	NPCR
1	Offered technique	33.2700	99.9820
2	Liu et al. [10]	33.4000	98.6000
3	Norouzi et al. [13]	33.5621	99.8067
4	Sam et al. [17]	33.4352	99.6159

6.11 Time Complexity Analysis

The total time in seconds carried by the suggested technique to be run depending on the input length is described as time complexity. The algorithm was executed on a personal computer with an Intel(R) for the simulations. Core (TM) i7-7500U 2.90 GHz CPU and 8 GB memory capacity. MATLAB R2019b was utilized for the simulations. The execution time (in seconds) of different sizes of Peppers image is depicted in Tab. 11.

Table 11: Time complexity analysis of the offered scheme

Image size	Execution time (in seconds)
128 × 128	1.45
256 × 256	2.79
512 × 512	3.31
1024 × 1024	5.91

7 Conclusion and Future Recommendations

In this work, we have designed an innovative image encryption technique by employing a discrete one-dimensional logistic map and a continuous convective atmospheric model (Lorenz chaotic system). The first phase of offered image encryption scheme involves the construction of a nonlinear confusion component of the block cipher. This S-box is fundamentally accountable for the confusion in the anticipated encryption mechanism. In the second phase, we have employed a Lorenz chaotic system as a diffusion agent in the offered technique. The obtained outcomes are then contrasted with previously existing benchmarks in image encryption methods. Our anticipated image encryption scheme has quite satisfactory statistical results.

The suggested encryption structure can also be turned into a lightweight mechanism by offering small 4 × 4 S-boxes with fractional chaotic logistic maps. The offered structure can be extended in audio and video encryption.

Data Availability Statement: The data utilized in this manuscript are available in the open SIPI Image Database at http://sipi.usc.edu/database/.

Funding Statement: The author Mohammad Mazyad Hazzazi extend his appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under Grant no. R.G.P. 2/150/42.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001. https://doi.org/10.1109/7384.963463.

[2] T. T. K. Hue, C. V. Lam, T. M. Hoang and S. A. Assad, "Implementation of secure SPN chaos-based cryptosystem on FPGA," in *IEEE Int. Symp. on Signal Processing and Information Technology (ISSPIT)*, Ho Chi Minh City, Vietnam, pp. 129–134, 2012. https://doi.org/10.1109/ISSPIT.2012.6621274.

[3] A. F. Webster and S. E. Tavares, "On the design of S-boxes," *Proceedings of Advances in Cryptology CRYPTO 85*, Springer, Berlin, Heidelber, vol. 218, pp. 523–534, 1986, [Online]. Available: https://doi.org/10.1007/3-540-39799-X_41.

[4] M. Lawnik, "Generalized logistic map and its application in chaos based cryptography," in *IOP Conf. Series: Journal of Physics, Conf. Series 936*, Pafos, Cyprus, pp. 1–4, 2017. https://doi.org/10.1088/1742-6596/936/1/012017.

[5] J. Munkhammar, "Chaos in fractional order logistic equation," *Fractional Calculus and Applied Analysis*, vol. 16, no. 3, pp. 511–519, 2013, [Online]. Available: https://doi.org/10.2478/s13540-013-0033-8.

[6] E. N. Lorenz, "Maximum simplification of the dynamic equations," *Tellus*, vol. 12, pp. 243–254, 1960, [Online]. Available: https://doi.org/10.1111/j.2153-3490.1960.tb01307.x.

[7] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, vol. 20, pp. 130–141, 1963, [Online]. Available: https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

[8] B. Saltzman, "Finite amplitude free convection as an initial value problem—I," *Journal of the Atmospheric Sciences*, vol. 19, pp. 329–341, 1962, [Online]. Available: https://doi.org/10.1175/1520-0469(1962)019<0329:FAFCAA>2.0.CO;2.

[9] X. Liao, S. Lai and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Sig Process*, vol. 90, no. 9, pp. 2714–2722, 2010, [Online]. Available: https://doi.org/10.1016/j.sigpro.2010.03.022.

[10] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, pp. 3895–3903, 2011.

[11] A. A. Abd El-Latif, L. Li, T. Zhang, N. Wang, X. Song *et al.,* "Digital image encryption scheme based on multiple chaotic systems," *Niu Sens Imaging*, vol. 13, pp. 67–88, 2012.

[12] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, 2015.

[13] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn*, vol. 78, pp. 995–1015, 2014.

[14] F. Masood, W. Boulila, J. Ahmad, S. Sankar, S. Rubaiee *et al.,* "A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos," *Remote Sensing*, vol. 12, no. 11, pp. 1893, 2020.

[15] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3D lorenz chaotic map," *Entropy*, vol. 22, no. 3, pp. 274, 2020.

[16] S. Arshad, M. Khan, I. Hussain "Pauli Half Spinning and Elliptic Curve Based Information Confidentiality Mechanism," *Journal of Theoretical Physics*, vol. 60, pp. 3631–3650, 2021.

[17] I. S. Sam, P. Devaraj and R. S. Bhuvaneswaran, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dyn*, vol. 69, pp. 1995–2007, 2012.
[18] S. I. Batool, M. Amin and H. M. Waseem, "Public key digital contents confidentiality scheme based on quantum spin and finite state automation," *Physica A: Statistical Mechanics and its Applications*, vol. 537, pp. 1–17, 2020.
[19] A. Alghafis, N. Munir, M. Khan and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *Journal of Theoretical Physics*, vol. 59, pp. 1227–1240, 2020, [Online]. Available: https://doi.org/10.1007/s10773-020-04402-7.
[20] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26203–26222, 2019.
[21] M. Khan, F. Masood and A. Alghafis, "Secure image encryption scheme based on fractals key with fibonacci series and discrete dynamical system," *Neural Computing and Applications*, vol. 32, pp. 11837–11857, 2020.
[22] N. Munir, M. Khan, T. Shah, A. S. Alanazi and I. Hussain, "Cryptanalysis of nonlinear confusion component based encryption algorithm," *Integration*, vol. 79, pp. 41–47, 2021.
[23] I. E. I. Hanouti, H. El Fadili, and K. Zenkouar, "Breaking an image encryption scheme based on arnold map and lucas series," *Multimed Tools Appl*, vol. 80, pp. 4975–4997, 2021, [Online]. Available: https://doi.org/10.1007/s11042-020-09815-4.
[24] N. Munir, M. Khan, S. S. Jamal, M. M. Hazzazi and I. Hussain, "Cryptanalysis of hybrid secure image encryption based on julia set fractals and three-dimensional lorenz chaotic map," *Mathematics and Computers in Simulation*, vol. 190, pp. 826–836, 2021.
[25] C. X. Zhu and K. H. Sun, "Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms," *Acta Physica Sinica*, vol. 61, no. 12, pp. 120503, 2012.