entropy

MDPI

*Article*

# A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map

**Fawad Masood [1], Jawad Ahmad [2], Syed Aziz Shah [3,*], Sajjad Shaukat Jamal [4] and Iqtadar Hussain [5]**

1 Department of Electrical Engineering, Institute of Space Technology, Islamabad Highway 1, Islamabad 44000, Pakistan; Fawadkttk@gmail.com
2 School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK; J.Ahmad@napier.ac.uk
3 School of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, UK
4 Department of Mathematics, College of Science, King Khalid University, Abha 62529, Saudi Arabia; shussain@kku.edu.sa
5 Department of Mathematics, Statistics, Physics, Qatar University, Doha 2713, Qatar; iqtadarqau@qu.edu.qa
* Correspondence: S.Shah@mmu.ac.uk

Received: 19 January 2020; Accepted: 23 February 2020; Published: 28 February 2020


**Abstract:** Chaos-based encryption schemes have attracted many researchers around the world in the digital image security domain. Digital images can be secured using existing chaotic maps, multiple chaotic maps, and several other hybrid dynamic systems that enhance the non-linearity of digital images. The combined property of confusion and diffusion was introduced by Claude Shannon which can be employed for digital image security. In this paper, we proposed a novel system that is computationally less expensive and provided a higher level of security. The system is based on a shuffling process with fractals key along with three-dimensional Lorenz chaotic map. The shuffling process added the confusion property and the pixels of the standard image is shuffled. Three-dimensional Lorenz chaotic map is used for a diffusion process which distorted all pixels of the image. In the statistical security test, means square error (MSE) evaluated error value was greater than the average value of 10000 for all standard images. The value of peak signal to noise (PSNR) was 7.69(dB) for the test image. Moreover, the calculated correlation coefficient values for each direction of the encrypted images was less than zero with a number of pixel change rate (NPCR) higher than 99%. During the security test, the entropy values were more than 7.9 for each grey channel which is almost equal to the ideal value of 8 for an 8-bit system. Numerous security tests and low computational complexity tests validate the security, robustness, and real-time implementation of the presented scheme.

**Keywords:** chaotic maps; confusion; diffusion; fractals; Lorenz chaotic maps; shuffling; non-linearity; hybrid dynamical system

## 1. Introduction

The application of multimedia information communication has grown dramatically in our daily lives. The multimedia data transmission necessitates high transmission rates and protection. The medical imaging systems, military image databases, and pay-per-view TV are such applications where preservation plays a fundamental role in the requirement of a multimedia system.

With the passage of time, we are increasingly encountering various kinds of vulnerabilities and security loopholes in wired and wireless communication media such as Wi-Fi, Ethernet, and so on. The digital world has changed the lives of human beings comparing it to earlier decades. The analogue transformation to digital bitstream was one of the groundbreaking discoveries of the well-known

scientist Claude Shannon in the year 1949, the same person introduced the property of confusion and diffusion. The property of randomness helped in securing digital multimedia information. The security of digital bitstream became one of the central issues when the data was transformed into a digital bitstream. The privacy of digital information posed a new problem in the digital world. The secure digital data in the form of binary bits are openly accessible for hackers. The data can be easily obtainable from the far site using the internet. It needs proper measurements to secure digital information over an insecure line of communication [1–3]. The digital data can be secured by hiding the identity of the original digital image over the secret cover image or another approach is pixels distortion or encryption. The first method of securing digital information is information hiding techniques and the study of steganography, which means the value of the data is preserved under the secret image. The image security is a very important issue as compared to textual security, where image pixels are to be examined concerning nearby pixels in a different orientation. The more pixels are dissimilar means the proposed encryption technique is more suitable for brute force attacks. Moreover, plain image pixels are always correlated to each other where an attacker can easily find secret information. Chaos-based encryption technique is preferred over some other existing methods because of less computational power, fast, and accurate. The future work is also extended to the direction of quantum-based cryptography, chaos quantum-based cryptography, and post-quantum random bit generators [4–12].

In the last few years, a large number of encryption algorithms schemes were proposed to secure the digital information from eavesdroppers and advertisers such as international data encryption algorithm (IDEA), data encryption standard (DES), and advanced encryption standard (AES) [13–22]. The foremost importance is given in implementing resolute protection while studying the hybrid properties of confusion and diffusion which was proposed by Claude Shannon as in [23,24]. Due to some of the major concerns including large data capacity, low entropy value and high correlation in the existing algorithms make it inappropriate for image encryption. The chaos-based encryption is a fast-growing area for image encryption. The use of chaotic maps, multiple chaotic maps, and hybrid dynamical systems of chaos-based encryption has attracted a large number of researchers and nowadays, the majority of scholars, researchers, and engineers are proposing security schemes based upon chaotic cryptography [25]. The highly pseudorandom sequences generated through chaotic maps provide strong entropy and least correlation between pixels of the ciphered image. Chaos-based encryption has brought the stretched gap between the plain and ciphered image which makes it challenging for invaders and attackers to break the code due to its robustness of the key generated through chaotic maps. Chaos-based encryption has certain unique properties which makes it superior over other approaches for encryption of plain digital images [11,26–29].

In addition, fractals are geometric shapes having non-linearity on all scales. It possesses randomness which makes it suitable for implementing secure and reliable cryptosystems. The system can be generated using the complex values of fractals in a complex domain. The chaotic nature of fractals using a private and public key is capable of securing digital multimedia information. The sensitivities and dependence on initial conditions produces complexities for an intruder to create the key to decipher the confidential information. The fractals generate infinitely complex patterns and show repetition and self-similarity at different scales. It is the repeating process of images and is familiar patterns since the whole universe consists of fractals in different forms [30–43]. In this context, we have designed a cryptosystem based on shuffling with Julia set of fractals key and chaos theory. The proposed algorithm at the stage of fractals generates random complex numbers for image encryptions. The complex numbers necessitate the extraction of real numbers to encrypt the plain image pixels. This system was secured with shuffling, but the histograms in the statistical section showed that the system can further be enhanced by the addition of chaotic maps providing the hybrid system. The fractals' random numbers are treated with the three-dimensional Lorenz chaotic map to gain robust security and validate all the security tests. The pair of histograms are shown in the subsequent section of the statistical tests. The statistical tests validated the proposed system.

The rest of the paper is composed as follows. Section 2 demonstrates the nonlinear mechanism and properties of the chaotic maps. In Section 3, the literature review of the work is addressed. Section 4 incorporates the methodology of the presented scheme. Section 5 elaborates the steps needed to develop a secure scheme. Section 6 will show the assessed results of the utilized secure algorithm and its comparison with already existing schemes. Section 7 covers the software and system specification needed to design the secure system. Finally, Section 8 is a brief discussion and conclusion of the paper by briefing the findings of the suggested cryptosystem.

## 2. Nonlinear Mechanism

A nonlinear process is a simple non-linear difference equation emerged in different fields of science—for instance in biology, physics, engineering, economics, and social sciences—which possess different dynamic behaviors which are pertinent to chaos or cryptography [44–48]. Chaos cryptography or chaotic systems have some properties for instance randomness nature, sensitive to the initial condition, aperiodic, and ergodicity which makes it unique for designing a secure cryptosystem. If the initial condition value is insignificantly changed the output at other ends will show immensely fickleness. Chaos behavior exists surrounding when looking into nature [49–55]. The basic schematic chart of image encryption is shown in Figure 1.

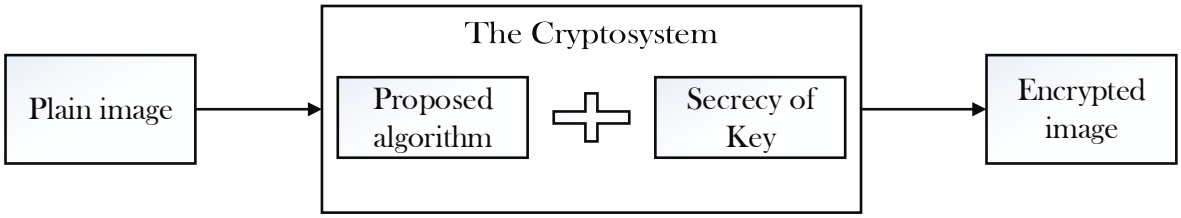



**Figure 1.** Basic schematic chart of image encryption.

*Properties of Chaotic Maps*

1. Deterministic: The chaotic maps are the deterministic dynamical non-linear systems. This means that if we recognize the initial condition, then the system can be determined easily else the system will behave chaotic unstable system [56].
2. Sensitivity to initial condition: The chaotic maps are highly sensitive to the starting condition of the system. The wrong keys will neither encrypt the image correctly nor decrypt the image properly. The change in the key will show highly strange attractors [56].
3. Randomness: The system will generate pseudorandom sequences. The sequences generated through chaos-based will be highly complex to be determined and prognosticated [30].
4. Unstable: The system will be unstable in the chaotic region. The Lyapunov exponent will determine the actual chaotic and non-chaotic regions [30].
5. Ergodicity of the chaotic maps: The encryption algorithm performance will have the same distribution for any plain text [30].

## 3. Literature Review

This section presented a literature review based on the existing algorithms for digital image encryption schemes. The basic operation is XOR which is used to encrypt the digital multimedia images for secure information. The XOR operation is bit by bit operation between binary numbers. The image can be decrypted by taking the XOR operation again. This is a very simple method to distort the pixels of the plain images.

In [57], the authors developed a scheme of encryption for digital multimedia information by experimental comparison of the chaotic and non-chaotic map. The cryptosystem used the discrete cosine transform, followed by Bernoulli map and permutation of pixels. The correlation coefficient

test, entropy, quality of encryption, avalanche effect, number of pixels changing rate unified average changing intensity, and key sensitivity test approved the proposed system. In [30], Masood et al. proposed a system based on Mandelbrot fractals and Fibonacci series followed by piecewise chaotic Kaplan–Yorke map. The hybrid system utilizing the Mandelbrot set of fractals generated the complex values. The real values are extracted from complex values and are treated with a chaotic map. The proposed system is investigated using different security tests for its validation. The system passed all the security tests and validated it for real-time communication. In [31], Agarwal introduced a system based on Mandelbrot fractals. The key generated by Mandelbrot fractals is further treated with discrete two-dimensional chaotic sequences. The system is followed by shuffling and complex *XOR* operation. The system is studied using specific statistical tests that authorized the suggested system. In [58], Batool et al. proposed a hybrid system based on image shuffling followed by pixel distortion. The pixels are initially shuffled using Arnold cat map for the channels of Lena and pepper as standard test images. The scrambled image is subjected to an encrypted phase where the pixels are distorted channel-wise. The Lucas sequence encrypted all the channels. The proposed system was validated using extensive experiments. Kumar et al. in [59] introduced a technicality entirely based on four-dimensional Lorenz chaotic map. The authors generated a random number matrix to improve security by using the hyperchaotic system. This method encrypted five different types of grey channel images including, the Mona Lisa test image, black, cameraman, vegetable, and rice. The proposed technique was passed through various tests to evaluate the validity of the system. The aforementioned encryption schemes can be applied on a number of different applications discussed in Refs [60–64].

## 4. Proposed Technique for Secure Cryptosystem

The main objective of the work is to determine a secure cryptosystem. In this communication, we initiated the designation of the system by the generation of fractals at a different value of $C$ and then utilized chaotic based three-dimension Lorenz system. The algorithm is investigated several times for different test images. The results of various statistical tests for different images are shown in the subsequent section of statistical parameters. The proposed system is valid for real time communication.

### *4.1. Initial Shuffling Process*

The grey channels red, green, blue (R, G, B) are initially randomly permuted to achieve the property of confusion. The shuffling process helped us obtaining partial security. however, the shape of the histograms of the shuffled grey channels looks same as the plain grey channels (R, G, B) and are shown in the subsequent section of statistical tests.

### *4.2. Julia Set of Fractals*

Julia's work is associated with a complex plane and the unique points for which the series generated through the $Z_{n+1} = Z_n^2 + C$ does not go to the infinity. The $C$ in the Julia set indicates the complex constant. The Julia fractals set changes with the change in the complex constant value $C$. The value must be smaller to generate Julia's set of fractals. The value of ($C < 1$) generates the desired quadratic based fractals. The different values of $C$ depicts different shapes of fractals [65]. The equation of quadratic Julia is the conformal mapping so in the case of conformal the angles are preserved. Suppose '$J$' be the Julia set then $x' \rightarrow x$ leaves $J$ invariant.

The quadratic Julia set of the system can be illustrated as

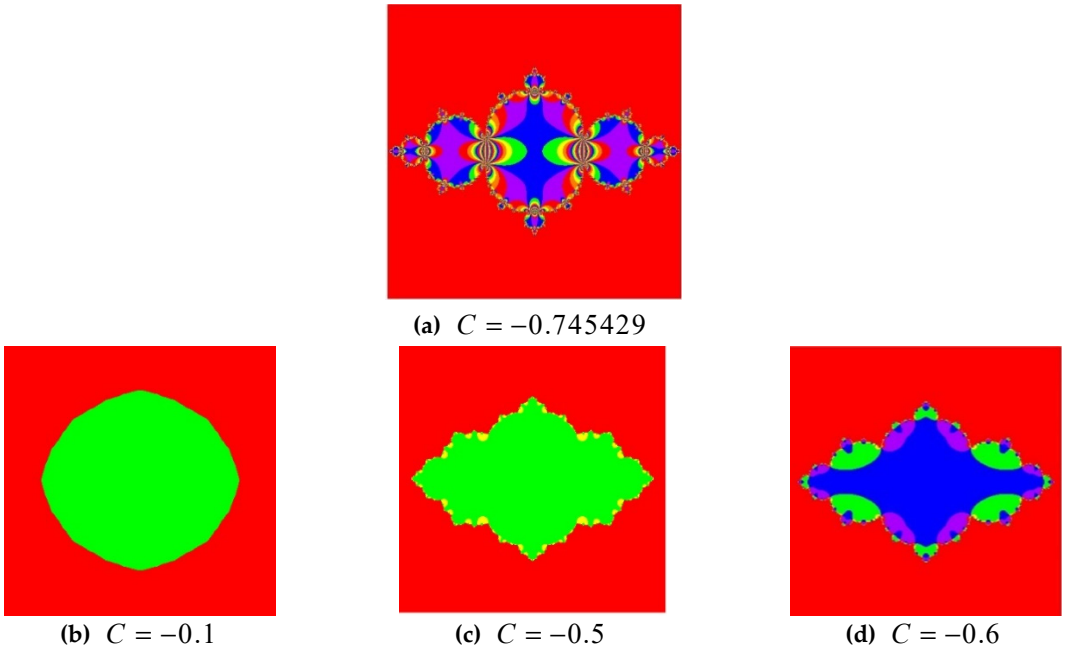
$$f(z) = z^2 + c \tag{1}$$

For almost every value of '$C$' will generate different types of fractals. The system behaves like chaos dynamical system by setting the value exact to $C = -0.745429$, and $C_x = 0$, $C_y = 0$.

The Julia set capacity dimension can be illustrated as

$$d_{capacity} = \frac{1 + |c|^2}{4 \ln 2} + O(|c|^3) \tag{2}$$

Different shapes of fractals are generated using Julia set of fractals with varying the value of $C$. The fractals give no shape when the value of ($C > 1$). The four distinct shapes of fractals are shown for the case of when ($C < 1$) as shown in Figure 2.



**(a)** $C = -0.745429$ **(b)** $C = -0.1$ **(c)** $C = -0.5$ **(d)** $C = -0.6$

**Figure 2.** Generated shapes (**a**–**d**) at ($C < 1$).

The complex shape of fractals is generated when the value of C is set to be = −0.745429. From Figure 2, it is clear that the proposed cryptosystem is secure.

### *4.3. Three-Dimension Chaotic Lorenz Map*

The Lorenz is a three-dimension chaotic dynamical map. The combined differential equation was developed by one of the notable scientist Edward Lorenz in 1963 [66]. The attractor generated through the Lorenz chaos sequences is the deck of chaotic solution for the Lorenz system. The plotting of the Lorenz system generates the attractor which looks like Butterfly. The chaotic system was initially developed for atmospheric convection. The system can be described using the simple formula

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x), \\ \frac{dy}{dt} &= rx - rz - y, \\ \frac{dz}{dt} &= xy - bz. \end{aligned} \tag{3}$$

The system majorly depends upon the control parameters, $r$, and $b$. The system produces chaos sequences when fixing the precise value of chaos. The trajectory of the system is achievable utilizing the Runga Kutta algorithm. The system presented chaos behavior and encrypt the channels for the rho (Rayleigh number) = 88500, (Sigma) = 10, and b (Beta) = 8/3. The system exhibited more excellent performance encrypting the channel wise images and appended the additional layer of security over the layer of fractal-based encrypted channels. The security of channels is reviewed here the advantage

of the Lorenz chaotic map and following the Lorenz chaotic map. The addition of Lorenz's chaotic map added much more randomness than fractals key-based encryption. The attractor that is generated by utilizing three dimensional Lorenz chaotic map is shown in Figure 3.

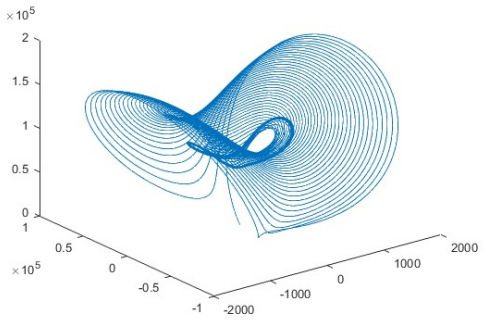



**Figure 3.** 3D Lorenz chaotic attractor.

## 5. A New Cryptosystem Based on Fractal Function and 3D Lorenz Chaotic Map

### *5.1. The Encryption Process*

1. The test image splash having the size of 512 × 512 × 3 is used for encryption on the suggested cryptosystem.
2. Convert the plaintext test image into three individual grey channels of red, green, and blue possessing the same size of 512 × 512.
3. Shuffle previously divided channel pixels to achieve partial security.
4. Produce the complex values from the complex domain of the Julia set of fractals.
5. Deduce the real values from the Julia set of fractals produced in step 4.
6. The real values of Julia's set of fractals are multiplied with the shuffled pixels in step 3.
7. Design three dimensional Lorenz chaotic map and bitwise XOR with output random stream of values that are generated in step 6.
8. Collect three highly random encrypted channels having a size of 512 × 512. Combine the three encrypted channels utilizing the cat command to produce a colored image having a size of 512 × 512 × 3.

### *5.2. The Decryption Process*

9. The colored encrypted image possessing a size of 512 × 512 × 3 is classified into three grey layers of encrypted channels (R, G, B) having a size of 512 × 512 sequentially.
10. Each channel is transferred through inverse by exerting bitwise XOR again for the three-dimensional Lorenz chaotic map to get the stream of values produced by Julia set of fractals.
11. The random values generated in step 6 of the encryption stage is classified by the Julia set of fractals.
12. The real values are now combined with the imaginary value to get the complex values of fractals.
13. In this step, the pixels are unshuffled to get into the respective grey channels with same size.
14. The grey channels having a size of 512 × 512 is combined using the cat command to get 512 × 512 × 3 full layered color image of a splash. The process of encryption and decryption and flow chart of the complete process is shown in the below Figures 4 and 5 respectively.

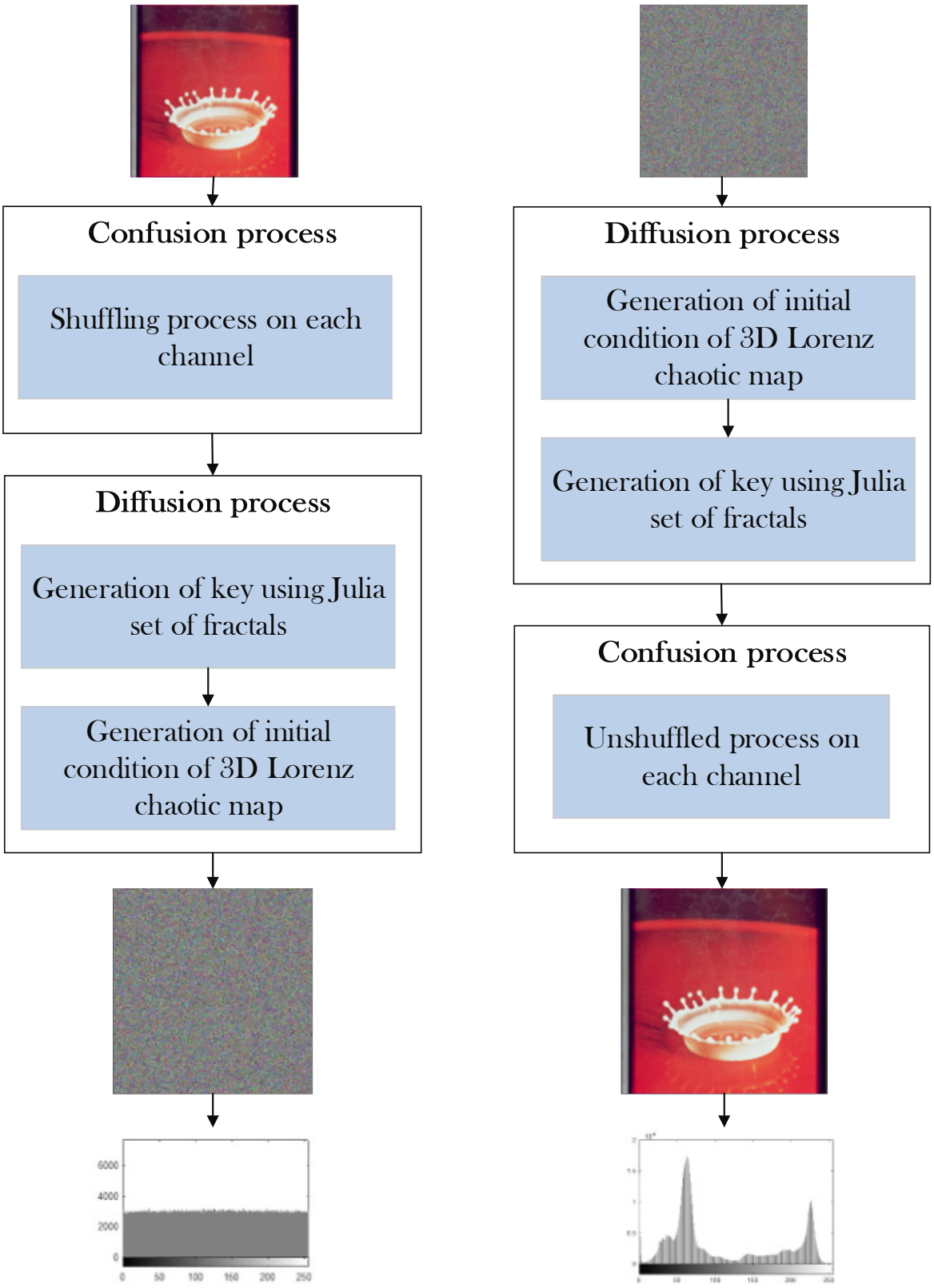



**Figure 4.** Encryption and decryption process.

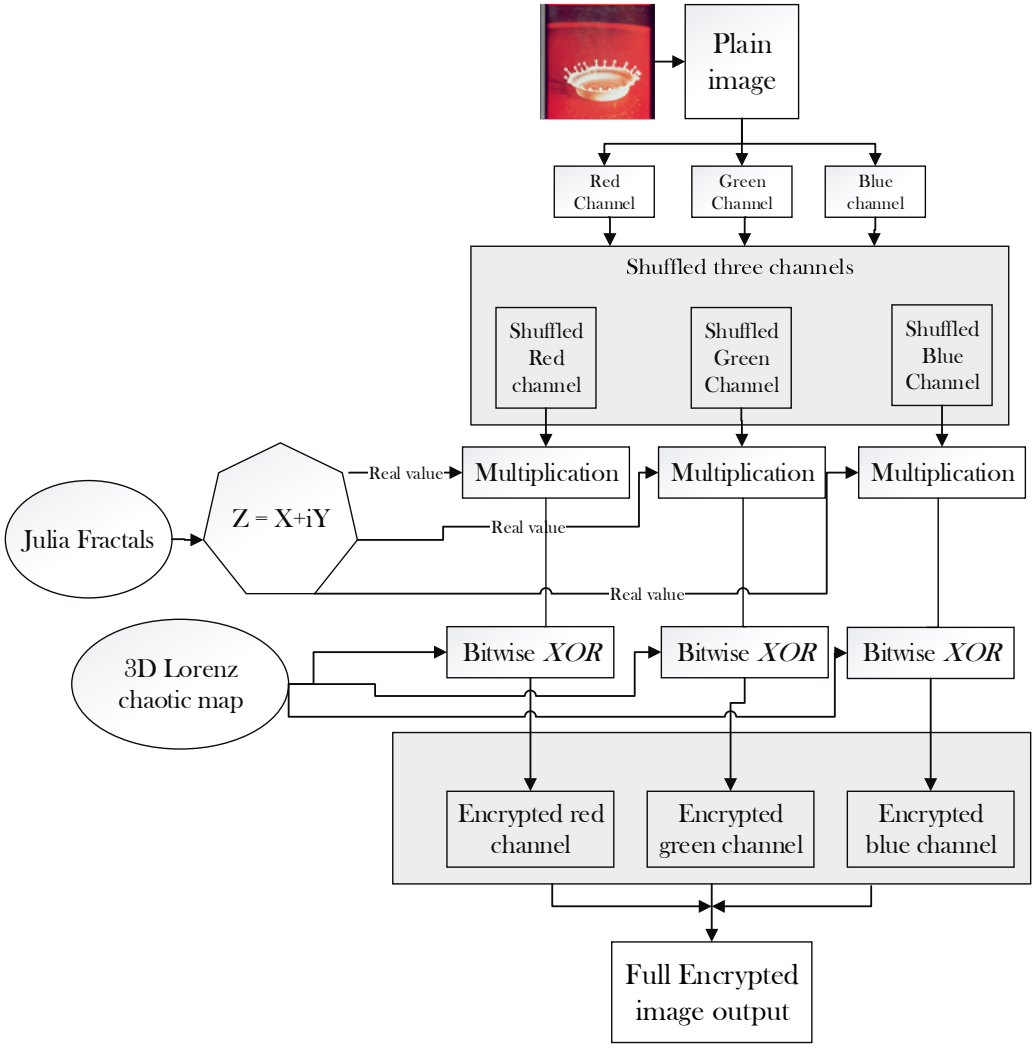



**Figure 5.** Flow chart for the proposed algorithm.

## 6. Security Evaluation of Proposed Scheme

The section comprises statistical tests that are implemented to the suggested hybrid system. The secure scheme is produced using a channel-wise shuffling process and is inserted to fractal function to produce the random bits. The random bitstream is then treated with the chaos-based 3D Lorenz dynamical systems. Some of the statistical tests are cumulated by using plain and encrypted images. The major tests include mean square error (MSE), peak to signal noise ratio (PSNR), mean absolute error (MAE), randomness test, number of pixels changing rate (NPCR), unified average changing intensity (UACI), and computational time. The following tests validated the proposed scheme. The analysis and security tests of pixels are performed in this section as shown subsequently in subsections.

In the below Figure 6a–d are the plain images of a splash having the original size of 512 × 512; while Figure 6e–h are the layer-wise splash images that are shuffled using Arnold map. The third column of Figure 6i–l are encrypted three layers of splash image which shows partial security during the process of image encryption using Julia set of fractals. In the subsequent Figure 7a–c are the plain images of splash while the partially secured channels are subjected to three dimensional Lorenz chaotic maps that improved the security level of the proposed scheme. Figure 7d–f are the fully secured encrypted three channels. Finally, full colored plain and encrypted image having a size of 512 × 512 × 3 are shown in Figure 8a,b. The proposed algorithm is utilized on several other images as well. In the following Figure 9a–d are the plain image of pepper with its three layers; while Figure 9e–h are the

shuffled full colored pepper image and its three layers. The encrypted three channels of pepper image which represents partial security during the process of image encryption using Julia set of fractals are shown in Figure 9i–l. The image is subjected to three dimensional Lorenz chaotic map. The high level of security is achieved after the additional layer of using Lorenz chaotic maps. In Figures 10a–c and 10d–f are the final plain and encrypted channels of pepper image. The full-dimensional colored plain and encrypted pepper image having a size of $512 \times 512 \times 3$ is shown in Figure 11a,b respectively. The Figure 12a–c are three plain layers of baboon images as shown; while the fully encrypted layers of baboon image of red, green and blue are shown in Figure 13a–c. The full colored plain and encrypted image of baboon having a size of $512 \times 512 \times 3$ are shown in Figure 14a,b.

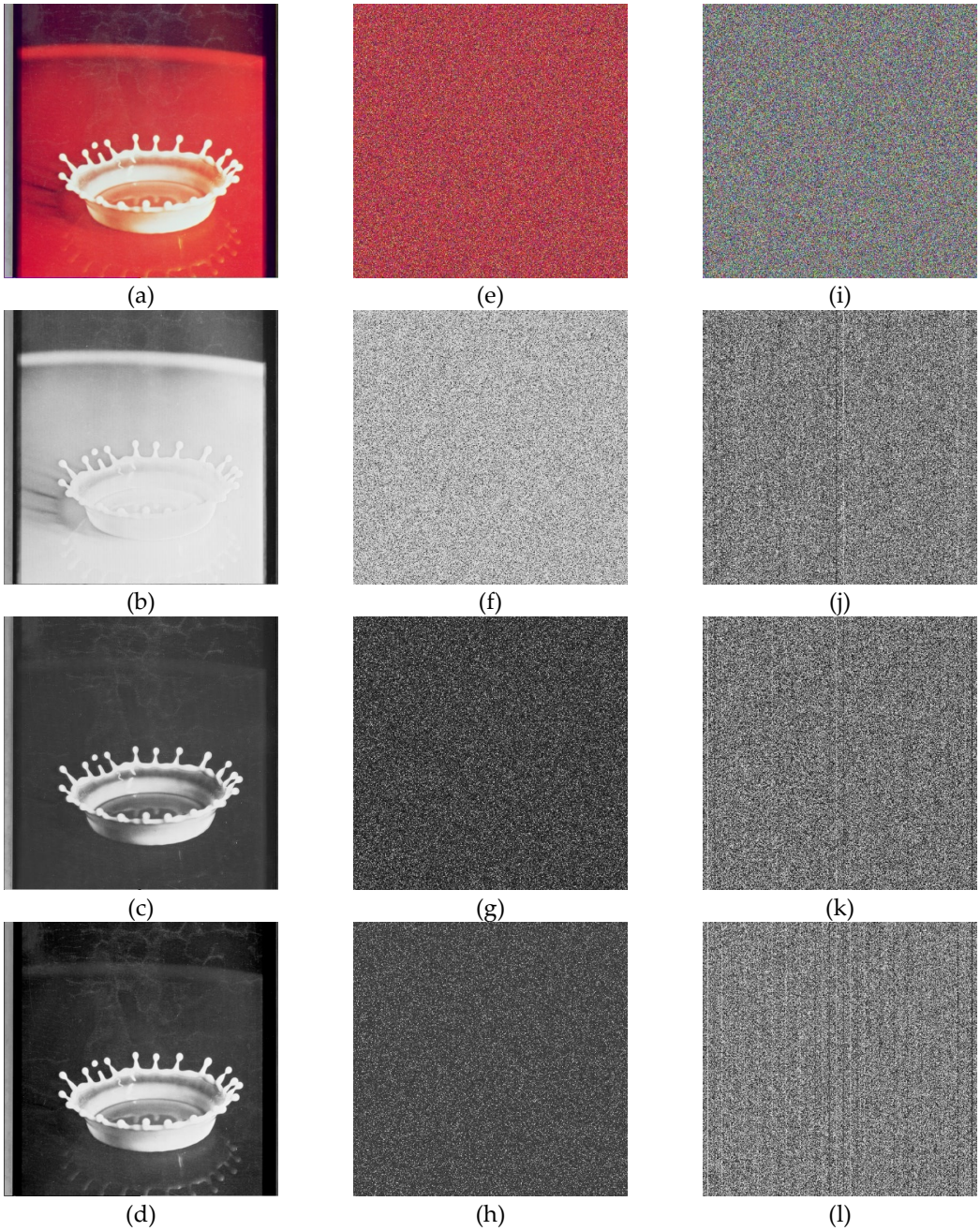



**Figure 6.** Plain and Encrypted images of splash ($512 \times 512$); (**a**–**d**) Plain image of splash and respected three channels of a splash test image. (**e**–**h**) Shuffled image of splash and respected three channels of splash image. (**i**–**l**) Encrypted image of splash and respected three channels of splash test images using Julia fractals.

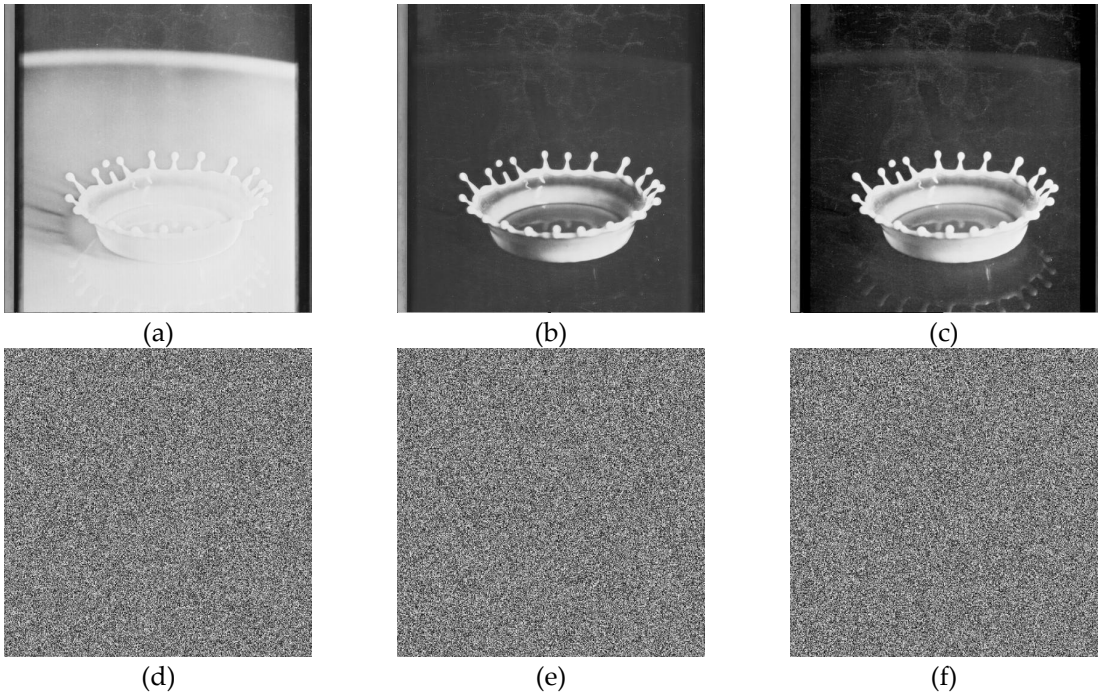



**Figure 7.** Plain and Encrypted images of splash (512 × 512); (**a**–**c**) Three respected plain channels of a splash test image. (**d**–**f**) The final encrypted channels using 3D Lorenz chaotic maps.

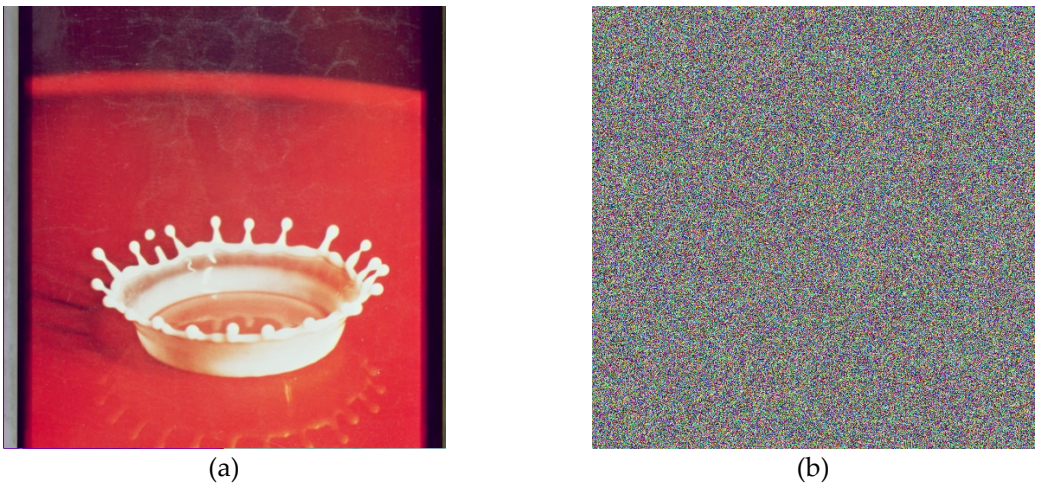



**Figure 8.** Plain and encrypted image of splash (512 × 512); (**a**) The plain image of a splash. (**b**) The final encrypted image of splash image using 3D Lorenz chaotic map.

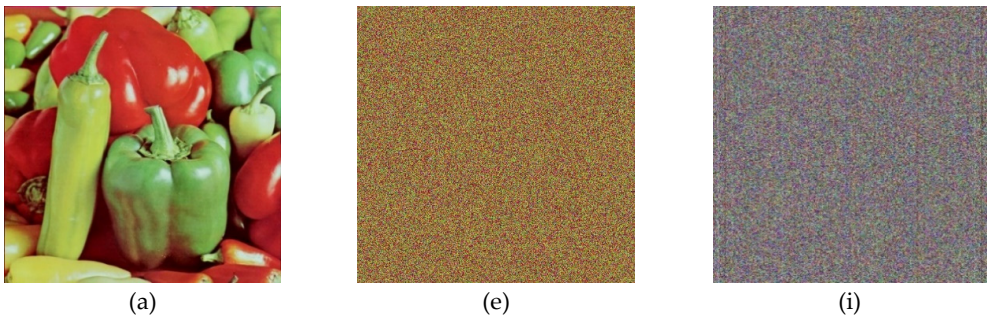



**Figure 9.** *Cont*.

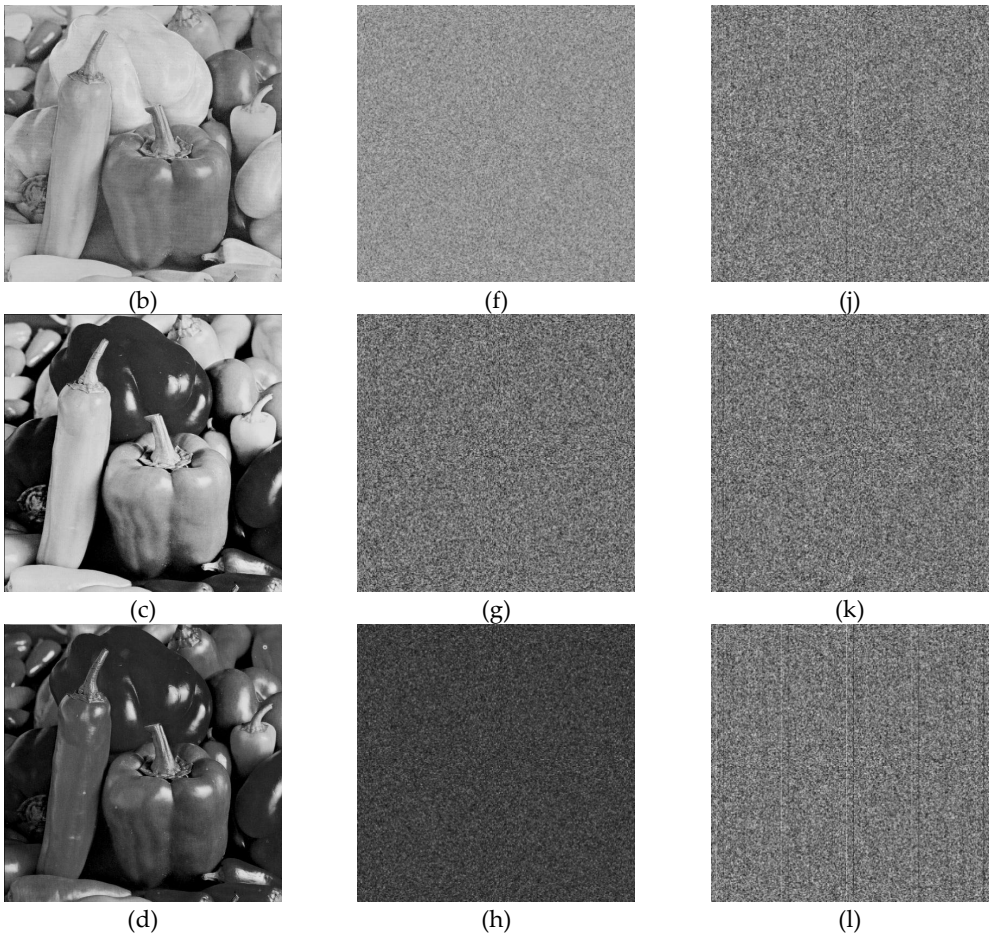


**Figure 9.** Plain and encrypted images of pepper (512 × 512); (**a**–**d**) Plain image of pepper and respected three channels of a pepper test image. (**e**–**h**) Shuffled image of pepper and respected three channels of pepper image. (**i**–**l**) Encrypted image of pepper and respected three channels of pepper test image using Julia fractals.

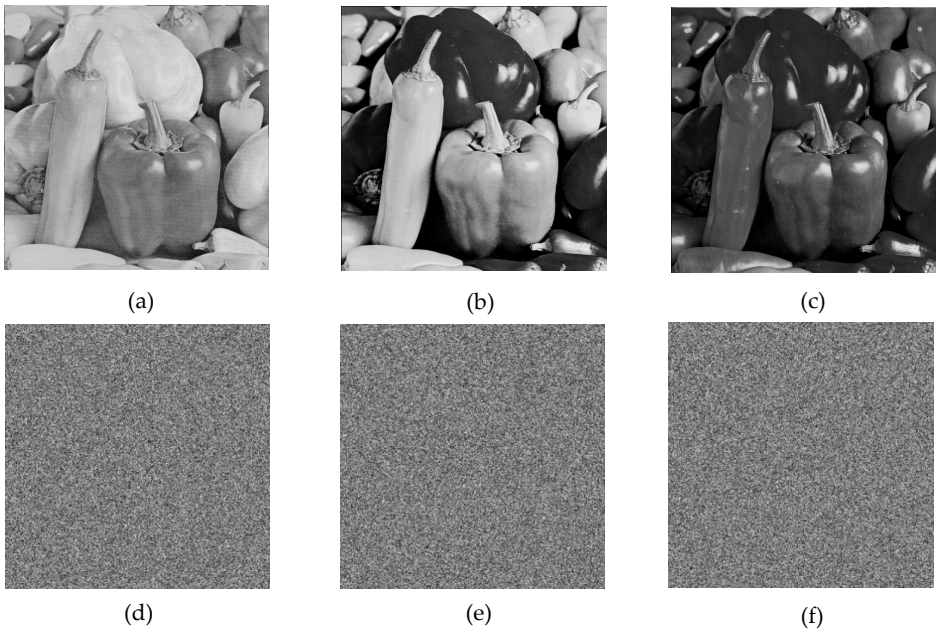
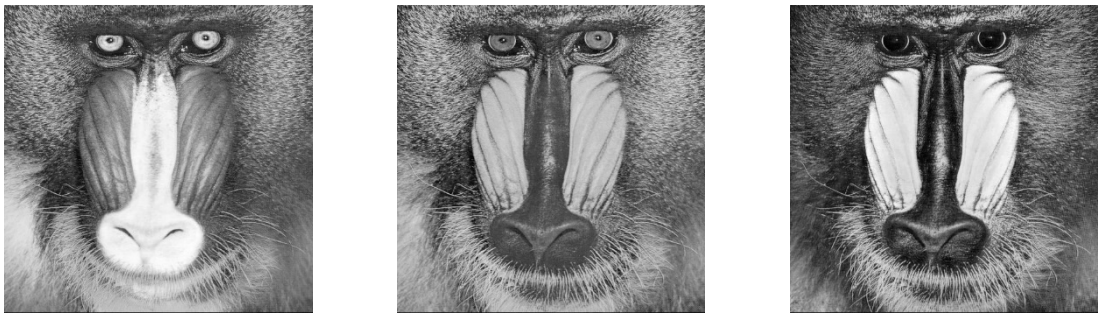


**Figure 10.** Plain and encrypted images of pepper (512 × 512); (**a**–**c**) Three respected plain channels of a pepper test image. (**d**–**f**) The final encrypted channels using 3D Lorenz chaotic maps.

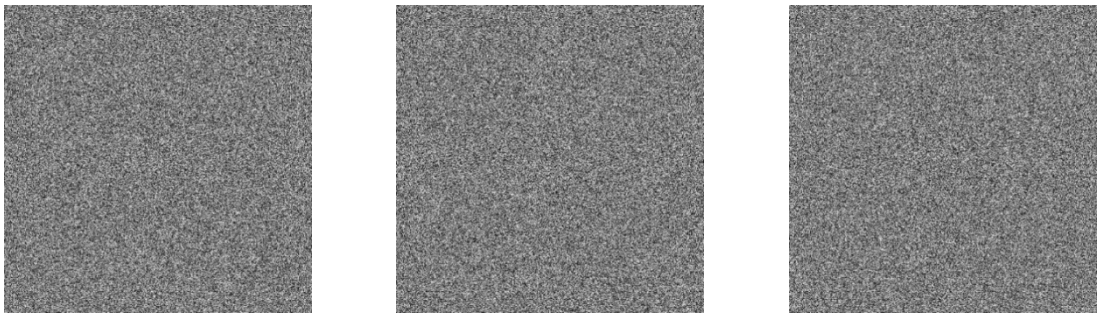
(a) (b)

**Figure 11.** Plain and Encrypted image of pepper (512 × 512); (**a**) The plain image of a pepper. (**b**) The final encrypted image of the pepper image using 3D Lorenz chaotic map.



(a) (b) (c)

**Figure 12.** Plain channel-wise test images of the baboon (512 × 512); (**a**–**c**) Three respected plain channels of a baboon test image.



(a) (b) (c)

**Figure 13.** Encrypted channel-wise test images of the baboon (512 × 512); (**a**–**c**) Three respected encrypted channels of a baboon test image using 3D Lorenz chaotic map.

(a) (b)

**Figure 14.** Plain and encrypted image of the baboon (512 × 512); (**a**) The plain image of a baboon. (**b**) The final encrypted image of the baboon image using 3D Lorenz chaotic map.

### *6.1. Histogram Analysis*

The histogram analysis is one of the most popular test that is used to estimate the robustness of the proposed cryptographic algorithm. The strength of the proposed scheme can be calculated by the distribution of pixels in its range. The minima and maxima range falls in 0–255 for 8-bit images. The up and down pixels in the plain image shows that the advertiser can attack the vulnerable bumpy pixels to guess the exact location of confidential information. The uniformity of pixels elaborates that confidential information is highly secured from any type of attack, thus the intruder is incapable of differentiating the pixels or guessing the quantity of information. It is essential to have uniform pixels for encrypted images. The up and down pixels show that the pixels did not achieve maximum randomness. The up and down pixels with minimum randomness reveals that the data is easily accessable. In Figure 15a–f the histograms of the three channels e.g., red, green, and blue depicts that the pixels information is insecure. The up and down pixels are breakable. In Figure 15g–l are the histograms of all the three respected channels of splash image are uniform that shows that the pixel information is secure and is not easily breakable. Finally, the whole colored plain and encrypted image having size of 512 × 512 × 3 are shown Figure 15m,n. The test is also applied on pepper image having the same size of 512 × 512 × 3. In Figure 16a–f are the histogram of three channels e.g., red, green, and blue. The non-uniform distribution of pixels reveals that the digital information is insecure for any type of communication. In Figure 16g–l are the histograms of secured channel when the images are subjected to secure cryptosystem. The Figure 16m,n is fully secured pepper image histogram for the combined three layers of colored image. The above information of histogram analysis demonstrate that the high level of security is achieved when the system is subjected to extra layer of chaotic map based on 3D lorenz system. The final channels wise histogram pixels in Figure 16j–l are smoothy distributed with no bumpy area. The above statements validated the suggested scheme.

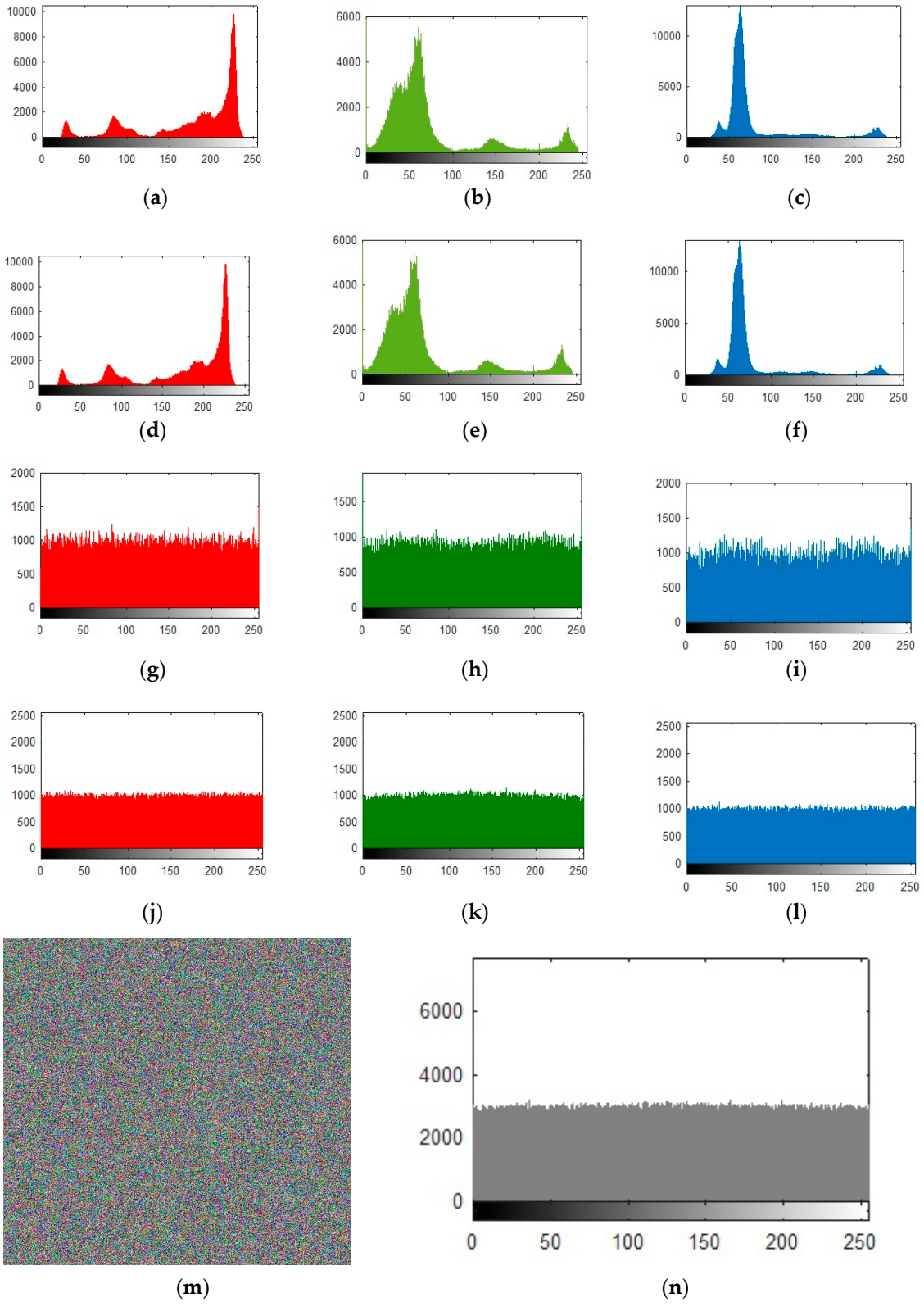



**Figure 15.** Plain and encrypted histogram of splash image (512 × 512); (**a**–**c**) Plain histograms for three grey channels of splash image. (**d**–**f**) Shuffled histograms for three grey channels of splash image. (**g**–**i**) Encrypted three channels of splash image using Julia fractals. (**j**–**l**) Final histograms of three channels using 3D Lorenz chaotic maps. (**m**,**n**) Final histogram of combined three channels for the splash test image.

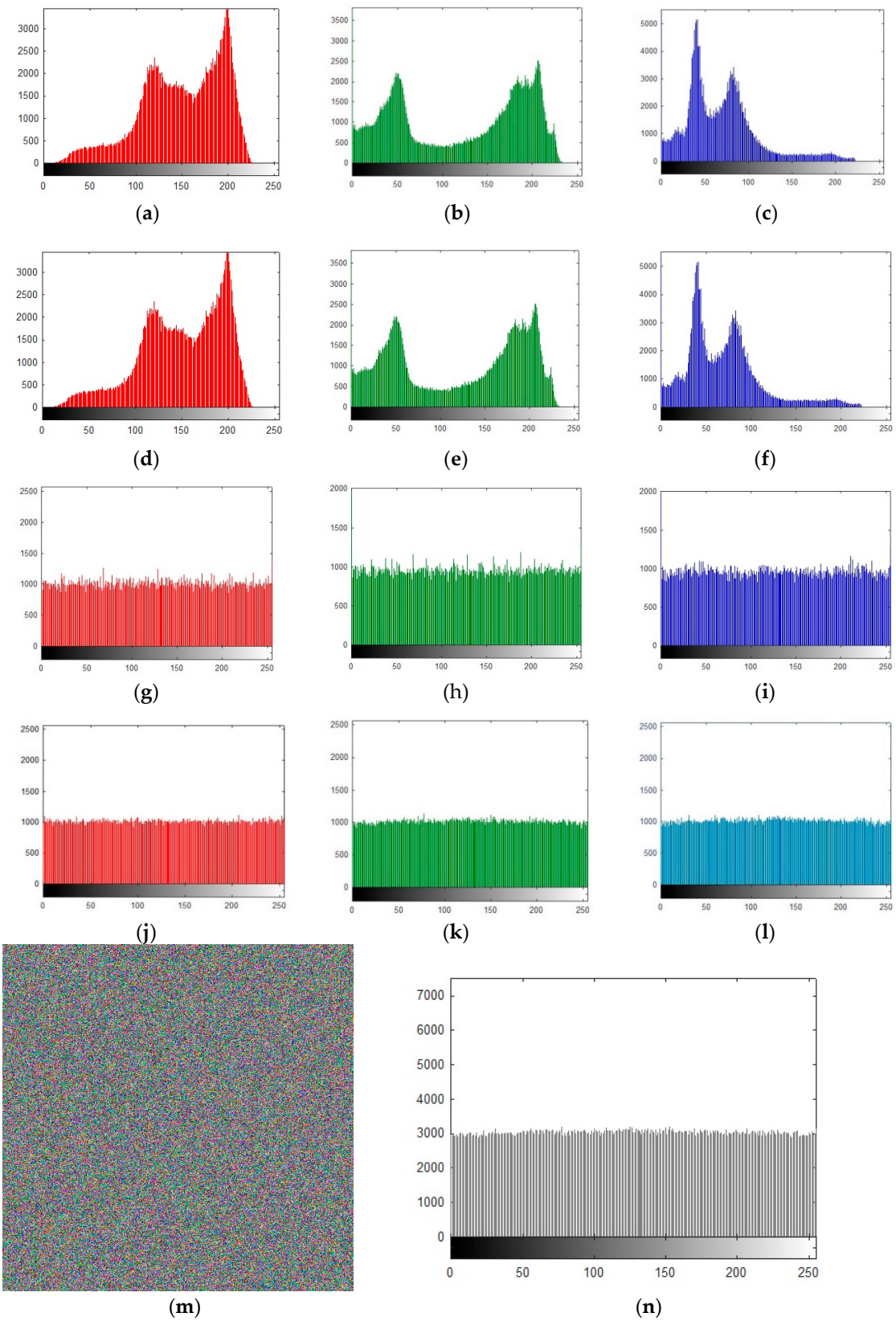



**Figure 16.** Plain and encrypted histogram of pepper image (512 × 512); (**a**–**c**) Plain histograms for three grey channels of pepper image. (**d**–**f**) Shuffled histograms for three grey channels of pepper image. (**g**–**i**) Encrypted three channels of pepper image using Julia fractals. (**j**–**l**) Final histograms of three channels using 3D Lorenz chaotic maps. (**m**,**n**) Final histogram of combined three channels for the pepper test image.

### *6.2. Correlation Analysis for the Adjacent Pixels*

The adjacent pixel analysis is also known as a correlation coffecient test which is one of the momentous tests to gauge the quality of encryption by relating the pair of variables. In this case, the pair of variables are plain text and ciphered text. The correlation coefficients take the value between two extreme points of [+1, −1]. The value that is nearing 1 explicates that the two-variable pixels are extremely dependent and there is an excellent correlation that survives between plain and ciphertext while the value of −1 shows the pair of variables are different from one another which explicates that there are highly dissimilarity exists. The value of 0 means that there is no relation between the two variables. In the case of perfect correlation, the two images are the same while in the case of getting the value of −1 reveals that the two images are distinct. The value must be small enough to gain satisfying security of the image. Mathematically, the correlation coefficient can be depicted as:

$$r = \frac{\mathrm{cov}(x, y)}{\sigma_X \times \sigma_y}, \tag{4}$$

where $\sigma_X = \sqrt{\mathrm{var}(x)}$ and $\sigma_y = \sqrt{\mathrm{var}(y)}$.

$$\mathrm{var}(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \tag{5}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \tag{6}$$

where $x$ and $y$ in the aforementioned equations are plain image pixels and encrypted image pixels whereas, $M \times N$ is the total dimension of the image. Figures 17 and 18 show the pixel distributions along with three directions of horizontal direction (H-D), vertical direction (V-D), and diagonal direction (D-D) pixels. The a–c in Figures 17 and 18 are the pixel distribution along three directions of splash and pepper images which are in the form of text possessing a dimension $512 \times 512 \times 3$. The pixels forming the diagonal lines depicts that the pixels are correlated to each other. The excessive amount of pixel's similarity is always in the high risk. Whereas in the case of Figures 17 and 18d–f the pixels are interspersed in the range of 0–256. The distribution of pixels covering the whole range shows that the values are highly dissimilar from each other which reveals that the cryptographic system is secure against attack.

Table 1 designates adjacent pixels values for three different directions. The system is investigated for six different test images possessing a dimension of $512 \times 512 \times 3$. The values of the plain image of splash for three different directions of horizontal, vertical, and diagonal are 0.9839, 0.9773, and 0.9913 which is imminent to the value of 1. The proposed splash image is encrypted and tested its pixels values dissimilarities along horizontal, vertical and diagonal directions are 0.0011, 0.0037, 0.0029 which is approaching 0 exhibits that the pixels are highly dissimilar from each other. Any type of attack is not possible on high non-correlated encrypted images.

Table 2 shows the comparison of the pixel's values in three different directions. The standard image of splash has corresponded to certain existing cryptosystems. The tests authorized the new hybrid based designed system and guaranteed that the designed cryptosystem is very strong compared to previously designed systems.

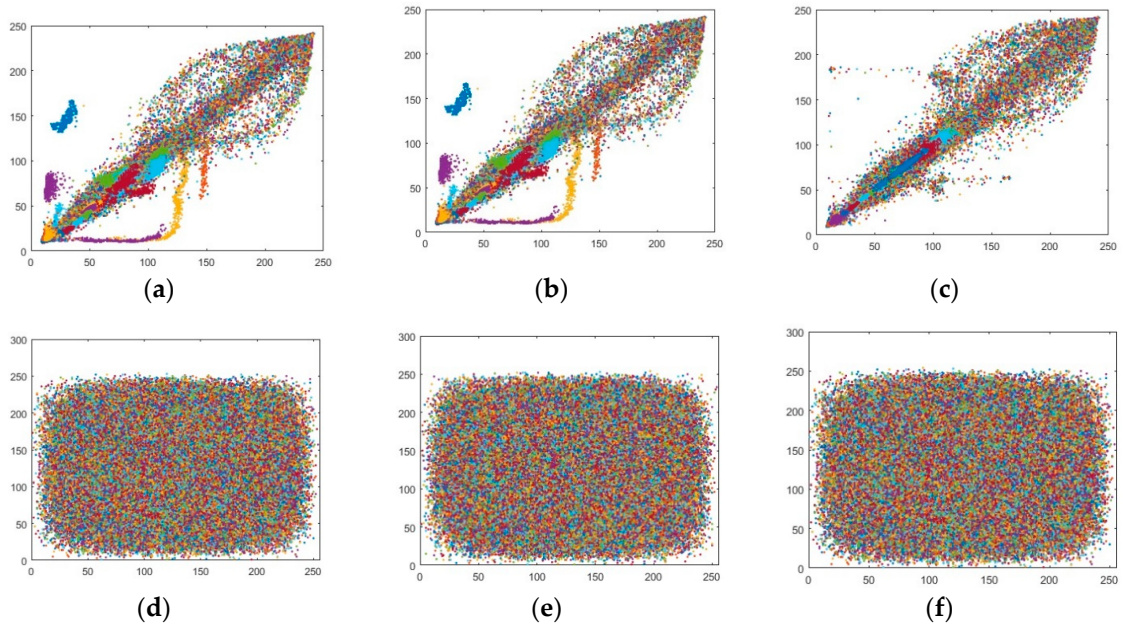


**Figure 17.** Correlation coefficient of splash image (512 × 512); (**a**–**c**) Correlation coefficient of plain splash image for three directions of a = Horizontal (H-D), b = Diagonal (D-D) and, c = Vertical (V-D). (**d**–**f**) Correlation coefficient of encrypted splash image for three directions of d = Horizontal (H-D), e = Diagonal (D-D) and f = Diagonal (V-D).

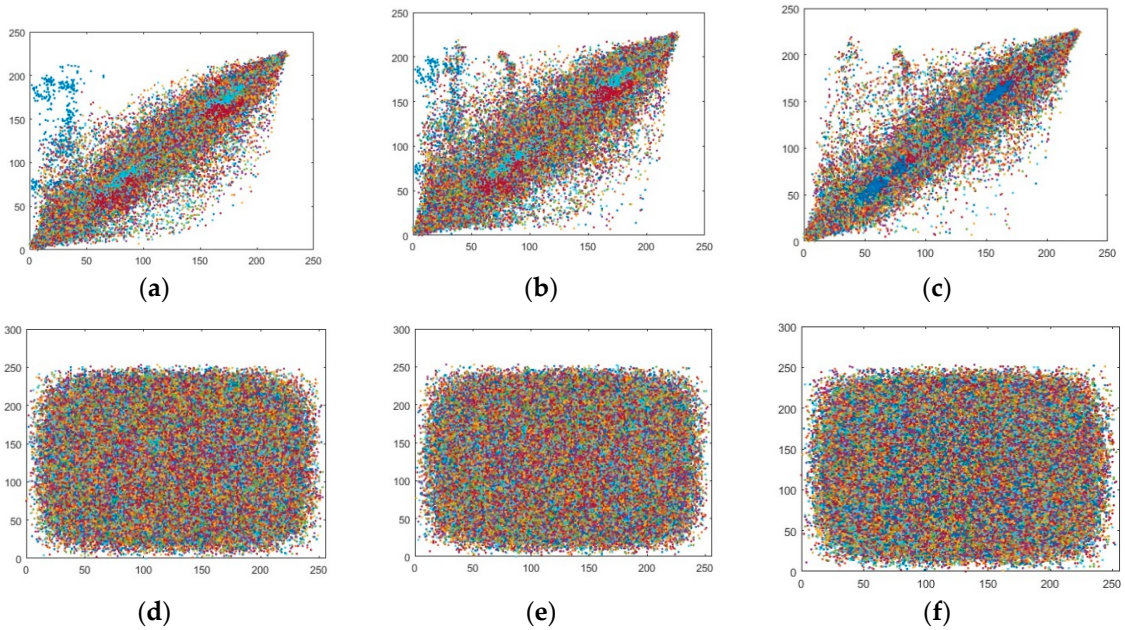


**Figure 18.** Correlation coefficient of pepper image (512 × 512); (**a**–**c**) The correlation coefficient of plain pepper image for three directions of a = Horizontal (H-D), b = Diagonal (D-D) and, c = Vertical (V-D). (**d**–**f**) The correlation coefficient of encrypted pepper image for three directions of d = Horizontal (H-D), e = Diagonal (D-D) and f = Vertical (V-D).

**Table 1.** Adjacent pixel correlation analysis test for different test images.

| | | Correlation Coefficient Directions | | | | | |
|---|---|---|---|---|---|---|---|
| | | Plain Image Directions | | | Ciphered Image Directions | | |
| **Image** | **Size** | **HD** | **DD** | **VD** | **HD** | **DD** | **VD** |
| Splash | 512 × 512 | 0.9839 | 0.9773 | 0.9913 | 0.0011 | 0.0037 | 0.0029 |
| Pepper | 512 × 512 | 0.9768 | 0.9639 | 0.9792 | −0.0009 | 0.0033 | 0.0008 |
| Tiffany | 512 × 512 | 0.9381 | 0.8943 | 0.9409 | 0.0002 | −0.0006 | 0.0057 |
| Airplane | 512 × 512 | 0.9663 | 0.9370 | 0.9641 | 0.0006 | −0.0011 | 0.0029 |
| Baboon | 512 × 512 | 0.8665 | 0.7262 | 0.7587 | −0.0038 | 0.0003 | 0.0007 |
| Fruit | 512 × 512 | 0.9738 | 0.9552 | 0.9743 | 0.0020 | 0.0022 | 0.0041 |

HD = Horizontal pixels direction, DD = Diagonal pixels direction, VD = Vertical pixels direction.

**Table 2.** Comparison of adjacent pixels with existing cryptosystems.

| | **Dimension** | **Correlation Coefficient Directions** | | |
|---|---|---|---|---|
| | | **HC** | **DC** | **VC** |
| Plain image | 512 × 512 | 0.9839 | 0.9773 | 0.9913 |
| Proposed | 512 × 512 | 0.0011 | 0.0037 | 0.0029 |
| Ref. [67] | 512 × 512 | 0.0075 | 0.0012 | 0.0049 |
| Ref. [68] | 512 × 512 | 0.0005 | 0.0008 | 0.0011 |
| Ref. [69] | 512 × 512 | 0.0117 | 0.0026 | 0.0010 |
| Ref. [70] | 512 × 512 | 0.0043 | 0.0054 | 0.0072 |
| Ref. [71] | 512 × 512 | 0.0108 | 0.0181 | 0.0061 |
| Ref. [72] | 512 × 512 | 0.0032 | 0.0042 | 0.0018 |
| Ref. [73] | 512 × 512 | 0.0204 | −0.0174 | 0.0231 |
| Ref. [74] | 512 × 512 | 0.0053 | −0.0027 | 0.0016 |

HC = Horizontal correlation, DC = Diagonal correlation, VC = Vertical correlation.

### *6.3. Mean Absolute Error*

This is one of the widely use standard analysis that is used to investigate the robustness of the proposed system. The value must be greater to validate the proposed scheme. The M × N is the cumulative dimension of the standard image. The $P_{i,j}$ is the plain image and $E_{i,j}$ is the encrypted image. The system can be illustrated as

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |E_{i,j} - P_{i,j}| \tag{7}$$

Table 3 consists of six standard test images. The analysis is applied to the encrypted images of the proposed system. It is important to accomplish a larger value to pass the test which confirms the robustness of the proposed cryptosystem. The standard test images of MAE values are displayed in the subsequent Table 3. The average value should be in the range of 65 to 70. The reliability of the system entirely depends on the greater value of MAE. The greater values depict that the attained cryptographic system has better resistivity against the differential attacks. Different values are calculated in the subsequent Table 3 for different standard images. The dimension of 512 × 512 for each test image is kept constant. The values are compared to already existing cryptosystems. The aforementioned information authenticated the proposed system.

**Table 3.** Mean absolute error (MAE) values and its comparison.

| Image | Dimension | MAE value | Ref. [75] | Ref. [56] |
|---|---|---|---|---|
| Splash | 512 × 512 | 76 | - | 76 |
| Pepper | 512 × 512 | 79 | 74 | 74 |
| Baboon | 512 × 512 | 175 | - | - |
| Tiffany | 512 × 512 | 183 | 76 | 94 |
| Airplane | 512 × 512 | 125 | 74 | - |
| Fruit | 512 × 512 | 211 | - | - |

### *6.4. Differential Attack Analysis*

Two types of tests are employed to attain sensitivity or differential attack analysis. The number of pixels changing rate (NPCR) and unified average changing intensity (UACI). These tests are used against differential attacks. The tests signify the chance of occurrence of the attack and its sensitivity towards the source image by changing the value. The tests are elaborated in the following subsection.

#### 6.4.1. Number of Pixel Changing Rate

The NPCR or number of pixel changing rate manifests the possibility of the differential attack by its sensitivity. The highly sensitivity of the system shows that the generated algorithm is sturdy against any probable attacks. The tests can be estimated by taking two encrypted images and one plain image. The variation in the encrypted images will occur with the change in the respected plain image. This shows that any petite change in the plain image will give an entirely different encrypted image. In simple words, it illustrates the percentage of the different pixels of encrypted images at the same position whose plain image is edited for the single pixel. The system can be calculated in percentage. The ideal value of NPCR is perpetually 100. The value approaching 100 shows that the proposed system is robust against any differential attack.

Let $E_1$ and $E_2$ be the two encrypted images whose source plain image is differed by a single pixel. The system is illustrated as

$$NPCR = \frac{\sum_{i,j} F(i,j)}{W \times H} \times 100\% \tag{8}$$

where $F_{i,j} = 0$ for $E_{1(i,j)} = E_{2(i,j)}$, and $F_{i,j} = 1$ for $E_{1(i,j)} \neq E_{2(i,j)}$.

Whereas $W \times H$ is the width and height (total size) of the image. In Table 4, the values of NPCR are calculated layer-wise for different standard test images having a size of 512 × 512. The computed values of NPCR ≥ 99.60. The value of splash red channel is = 99.62, the value of green channel is = 99.61 and the value of blue channel is = 99.62 with an average = 99.62. The results demonstrate that the system is near to the ideal value which is 100. The system has guaranteed that the designed system is applicable for real-time communication.

#### 6.4.2. Unified Average Changing Intensity

Unified average changing intensity (UACI) is one of the important analysis of sensitivity tests. It is mandatory to have robust security. The test is based upon the intensity difference between two images. The system can be computed using the equation

$$UACI = \frac{1}{W \times H} \sum_{i,j} \left[ \frac{E_{1(i,j)} - E_{2(i,j)}}{255} \right] \times 100\% \tag{9}$$

whereas the $W \times H$ is the cumulative size of the standard image. $E_1$ and $E_2$ are two encrypted images at $i$th row and $j$th column. The test is applied to three different encrypted images having a size of 512 × 512 channel-wise. The average value of UACI is 33 while the computed UACI values of standard

splash image value is 33.90, Tiffany obtained value is 36.26 and, airplane is equal to 32.50 as shown in Table 4.

In Table 5, the proposed encrypted image UACI value is compared to several existing secure system values. The proposed value of UACI is superior over the existing cryptosystems. The test ensured the proposed system values are highly satisfying the security criteria. The proposed system is valid for any type of secure communication.

**Table 4.** Layer wise NPCR and UACI values of standard images.

| | | | **Projected Technique** | |
|---|---|---|---|---|
| **Image** | **Channels** | **Dimension** | **NPCR** | **UACI** |
| Splash | R-L | 512 × 512 | 99.62 | 33.90 |
| | G-L | 512 × 512 | 99.61 | 33.90 |
| | B-L | 512 × 512 | 99.62 | 33.90 |
| Tiffany | R-L | 512 × 512 | 99.61 | 36.26 |
| | G-L | 512 × 512 | 99.61 | 36.26 |
| | B-L | 512 × 512 | 99.60 | 36.26 |
| Airplane | R-L | 512 × 512 | 99.62 | 32.03 |
| | G-L | 512 × 512 | 99.61 | 33.05 |
| | B-L | 512 × 512 | 99.62 | 32.66 |

**Table 5.** Comparison of NPCR and UACI proposed cryptosystem and its comparison.

| | **Average NPCR** | **Average UACI** |
|---|---|---|
| Proposed algorithm | 99.62 | 33.90 |
| Ref. [76] | 99.52 | 26.79 |
| Ref. [77] | 99.58 | 33.37 |
| Ref. [78] | 99.59 | 17.60 |
| Ref. [79] | 99.60 | 33.23 |
| Ref. [80] | 99.60 | 28.13 |
| Ref. [81] | 99.55 | 33.40 |
| Ref. [82] | 99.59 | 33.46 |

### *6.5. Mean Square Error*

It is important to have accuracy in the proposed system. The system without accuracy confronts different types of external attacks. The mean square error (MSE) test is used to find the accuracy of the suggested system by using the plain and encrypted images of the proposed system. The system can be computed as

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left( O_{(i,j)} - E_{(i,j)} \right) \tag{10}$$

Mean square error (MSE) must be greater in value to resist differential attack. The greater value of MSE shows that the proposed system is robust against any type of attack. The cryptographic algorithm has been investigated on various standard images to confirm the validity of the proposed scheme. In the subsequent paragragh, the calculated values are tabulated for six different standard images including the proposed image of splash.

In Table 6 The MSE values for the standard proposed test image of splash is investigated. The computed red layer is value is 11412.96, the value of green layer is 12272.97 and the value of blue layer is 9908.84. The secure system is investigated on several other test images. The average value of

11198.25 for the splash image is much greater than the average value of 10000. The average value of the pepper is 10842.43, the computed value of the baboon is 10905.36, the tiffany image value is equal to 12743.12, the evalauted fruit image value is 10034.06, and the airplane image is 10347.71. The result indicates that the proposed system is checked layer-wise and in the combined state.

**Table 6.** MSE and PSNR values of different layers for different standard images.

| Image | Dimension | | Projected Technique | |
|---|---|---|---|---|
| | | | **MSE** | **PSNR** |
| Splash | 512 × 512 | R-L | 11412.96 | 7.59 |
| | 512 × 512 | G-L | 12272.97 | 7.28 |
| | 512 × 512 | B-L | 9908.84 | 8.20 |
| Pepper | 512 × 512 | R-L | 10926.92 | 7.78 |
| | 512 × 512 | G-L | 10809.52 | 7.83 |
| | 512 × 512 | B-L | 10790.86 | 7.83 |
| Baboon | 512 × 512 | R-L | 10917.79 | 7.78 |
| | 512 × 512 | G-L | 10889.19 | 7.79 |
| | 512 × 512 | B-L | 10909.10 | 7.79 |
| Tiffany | 512 × 512 | R-L | 17689.78 | 5.69 |
| | 512 × 512 | G-L | 13128.56 | 6.98 |
| | 512 × 512 | B-L | 07411.03 | 9.47 |
| Fruit | 512 × 512 | R-L | 11119.78 | 7.70 |
| | 512 × 512 | G-L | 09904.70 | 8.21 |
| | 512 × 512 | B-L | 09077.72 | 8.59 |
| Airplane | 512 × 512 | R-L | 09969.32 | 8.18 |
| | 512 × 512 | G-L | 10663.63 | 7.89 |
| | 512 × 512 | B-L | 10410.19 | 7.99 |

In Table 7 the proposed image also compared to various exisiting schemes e.g., AES, AES-CBC, AES-Counter, AES-Feedback, AES-Stream.

**Table 7.** Comparison of existing MSE values with proposed cryptosystem.

| Algorithms | MSE values comparisons |
|---|---|
| AES | 4600 |
| AES-CBC | 4637 |
| AES-Counter | 4938 |
| AES Feedback | 4577 |
| AES-Stream | 4911 |
| Proposed | 11198 |

### *6.6. Peak to Signal Noise Ratio*

Peak to signal noise ratio is an important analysis for the suggested system to evaluate the quality of the image. The system can be illustrated as

$$PSNR = 10 \log_2 \frac{I_{\max}^2}{MSE} \tag{11}$$

The value of mean square error (MSE) and peak to signal noise ratio (PSNR) is always inversely to each other. The ample value of MSE with its lower value of PNSR signifies good security. The values of a peak to signal noise ratio (PSNR) for the splash image for a red layer is 7.59, green layer is 7.28, and a blue layer is 8.20 as shown in Table 6.

The results are tabulated in Tables 6 and 8. The values of PSNR is evaluated for all the three channels for certain standard images is shown in Table 6. In Table 8 the average values are tabulated for mean square error (MSE) and peak to signal noise ratio (PSNR); the average calculated value of splash image is 7.69, following the average evaluated value of pepper image is 7.81, the value of baboon image is 7.79, similarily the tiffany is 7.38, the fruit image is equal to 8.16, and finally 8.08 is calculated value of airplane standard test image.

**Table 8.** Average mean square error (MSE) and peak to signal noise ratio (PSNR) value.

| | **Projected Technique** | |
|---|---|---|
| | **Average MSE** | **Average PSNR** |
| Splash | 11198.25 | 7.69 |
| Pepper | 10842.43 | 7.81 |
| Baboon | 10905.36 | 7.79 |
| Tiffany | 12743.12 | 7.38 |
| Fruit | 10034.06 | 8.16 |
| Airplane | 10347.71 | 8.02 |

The results in Tables 6 and 8 indicates that the proposed system values are remarkable compared to already systems developed to date. The system has ensured the strongness against brute force attacks.

### *6.7. Entropy*

Information entropy is a powerful analysis used to find the unpredictability and randomness in the suggested scheme. The important term was originally used by the notable scientist, Claude Shannon, for the first time in 1949 [43]. It is also known as Shannon entropy of randomness which is used to find the quality of encryption in the proposed system. The ideal value is always equal to 8 for which the pixel values of the image always fall in the range of 0–255. The entropy value may fluctuate for the various pixel values of the image falls. Hence the suggested cryptosystem has 256 states so the maximum information entropy will be approached to 8. The information entropy 'm' can be estimated by utilising the formula as

$$H(m) = \sum_{i=0}^{2^K-1} p(m_i) \log_b(1/p(m_i)) \tag{12}$$

whereas $p(m_i)$ is the probability of the message 'm', the $2^K$ in the above equation is the number of possible outcomes for the number of bits 'K' included for each message. The entropy values are evaluated for different standard images having a size of $512 \times 512 \times 3$ and channels wise having a size of $512 \times 512$. The value must be nearer to the ideal value of 8.

In Table 9 layer-wise entropy tests are applied for each encrypted image. The test is applied to eight different images. The topmost two images of splash and pepper are considered as the proposed standard images whilst the test is applied for remaining images as well. The values of 7.9992, 7.9991, 7.9993 for red, green, and blue channels of the proposed splash image is almost equal to 8. The test is further applied to the proposed standard test image of peppers having entropy values of red, green, and blue is 7.9993. The rest of the results are remarkable as shown below.

In Table 10 the combined values are calculated for eight standard images. The values of 7.9997 and 7.9998 reveal that the system has much randomness. In Table 11 the proposed system is compared to several eight types of already existing entropy values. The highly random values are difficult to be breakdown against any attack.

**Table 9.** Information entropy analysis for each respective channel.

| | | Encrypted Channels | | |
|---|---|---|---|---|
| **Images** | **Dimension** | **Red Channel** | **Green Channel** | **Blue Channel** |
| Proposed 1 | 512 × 512 | 7.9992 | 7.9991 | 7.9993 |
| Proposed 2 | 512 × 512 | 7.9993 | 7.9993 | 7.9993 |
| Baboon | 512 × 512 | 7.9993 | 7.9993 | 7.9992 |
| Tiffany | 512 × 512 | 7.9993 | 7.9994 | 7.9993 |
| Airplane | 512 × 512 | 7.9994 | 7.9994 | 7.9994 |
| Fruit | 512 × 512 | 7.9993 | 7.9993 | 7.9993 |
| Pepper | 512 × 512 | 7.9993 | 7.9993 | 7.9993 |
| Lena | 512 × 512 | 7.9994 | 7.9993 | 7.9994 |

**Table 10.** Cumulative entropy values for certain test images.

| **Test Images** | **Dimension** | **C-M Entropy** |
|---|---|---|
| Ideal value | 512 × 512 × 3 | 8.0000 |
| Proposed 1 | 512 × 512 × 3 | 7.9997 |
| Proposed 2 | 512 × 512 × 3 | 7.9998 |
| Baboon | 512 × 512 × 3 | 7.9997 |
| Tiffany | 512 × 512 × 3 | 7.9998 |
| Airplane | 512 × 512 × 3 | 7.9998 |
| Fruit | 512 × 512 × 3 | 7.9998 |
| Pepper | 512 × 512 × 3 | 7.9998 |
| Lena | 512 × 512 × 3 | 7.9998 |

C-M = Commulative measured.

**Table 11.** Comparison of proposed and Lena value with certain existing entropy values.

| **Images** | **Dimension** | **Entropy Values** |
|---|---|---|
| Proposed | 512 × 512 × 3 | 7.9997 |
| Lena | 512 × 512 × 3 | 7.9998 |
| Ref. [83] | 512 × 512 × 3 | 7.996 |
| Ref. [84] | 512 × 512 × 3 | 7.997 |
| Ref. [85] | 512 × 512 × 3 | 7.989 |
| Ref. [86] | 512 × 512 × 3 | 7.997 |
| Ref. [87] | 512 × 512 × 3 | 7.997 |
| Ref. [88] | 512 × 512 × 3 | 7.993 |
| Ref. [89] | 512 × 512 × 3 | 7.998 |
| Ref. [22] | 512 × 512 × 3 | 7.997 |

### *6.8. Time Complexity*

It is important to propose an efficient system. The system without efficiency has no value. The proposed system must be computationally fast and execution time takes fewer seconds to encrypt the channels and then for the full image as well. The proposed algorithm is tested on six test images and the execution time is noted for when the system encrypts the 512 × 512 channel and then encrypts the whole channel of 512 × 512 × 3. The time complexity test is done on the core i5 system having AMD Radeon graphics with 8 Gb ram. The proposed system in Table 12 shows that the system is much efficient. The unique system always takes the same time for encryption and decryption. The proposed cryptosystem is validated by the time complexity test.

**Table 12.** Time complexity analysis for certain images.

| Images | Dimension | Proposed Schemes | Ref. [53] | Ref. [90] |
|---|---|---|---|---|
| Splash | $512 \times 512$ | 1.291540 | - | - |
| Pepper | $512 \times 512$ | 0.636624 | 2.76 | 3.68 |
| Tiffany | $512 \times 512$ | 1.302140 | - | - |
| Airplane | $512 \times 512$ | 1.059419 | - | - |
| Fruit | $512 \times 512$ | 1.098649 | - | - |
| Baboon | $512 \times 512$ | 0.609787 | 2.55 | 3.53 |

## 7. Software and System Specification

The tests are performed for several test images having the size of $512 \times 512 \times 3$ using the MATLAB 2017(a) version and workstation of ASUS CPU Core $i5^{TM}$(fourth generation) 8gb ram, AMD Radeon Graphics. The OS of the workstation is Windows 10.

## 8. Conclusions

The paper proposed a hybrid chaotic fractal system consisting of fractal function and chaos-based three-dimensional chaotic map. The standard image was shuffled channel-wise prior to encryption. The encryption phase scrambled layer-wise images based on the multiplication operation using the Julia set of fractals. Furthermore, the encrypted layers are passed through the bitstream of the 3D Lorenz chaotic dynamical map for achieving higher security. The results of the proposed scheme were compared with existing secure algorithms. The addition of confusion and diffusion steps enhanced the robustness of the system when compared with traditional algorithms. The experimental analysis demonstrates that the suggested system indicated high sensitivity to initial conditions, strange attractor, aperiodicity, low correlation coefficient, high mean square error, and low peak to signal-noise ratio. The NPCR and UACI tests show that the proposed system is highly sensitive to a slight change in the plain image. The above security parameters have verified the proposed system for real-time communication. The proposed cryptosystem will be modified and tested for audio and video communication in the future.

**Author Contributions:** Conceptualization, F.M., J.A., S.A.S.; Data curation, S.A.S., F.M.; Methodology, Fawad Masood Validation, S.A.S., J.A.; Investigation, I.H., F.M.; Formal Analysis, J.A., F.M., S.A.S.; Resources, writing, review and editing J.A., F.M., S.S.J. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Acknowledgments:** The author Sajjad Shaukat Jamal extend his appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under grant number R.G.P. 2/58/40.

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

## References

1. Ahmad, J.; Ahmed, F. Efficiency analysis and security evaluation of image encryption schemes. *Computing* **2010**, *23*, 18–31.
2. Younas, M.B.; Ahmad, J. Comparative analysis of chaotic and non-chaotic image encryption schemes. In Proceedings of the 2014 International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, 8–9 December 2014.
3. Khan, M.; Masood, F. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimed. Tools Appl.* **2019**, *78*, 26203–26222. [CrossRef]
4. Kaur, M.; Kumar, V. A comprehensive review on image encryption techniques. *Arch. Comput. Methods Eng.* **2018**, *27*, 15–43. [CrossRef]
5. Waseem, H.M.; Khan, M. A new approach to digital content privacy using quantum spin and finite-state machine. *Appl. Phys. B* **2019**, *125*, 27. [CrossRef]

6. Khan, M.; Waseem, H.M. A Novel Digital Contents Privacy Scheme Based on Kramer's Arbitrary Spin. *Int. J. Theor. Phys.* **2019**, *58*, 2720–2743. [CrossRef]
7. Rafiq, A.; Khan, M. Construction of new S-boxes based on triangle groups and its applications in copyright protection. *Multimed. Tools Appl.* **2019**, *78*, 15527–15544. [CrossRef]
8. Younas, I.; Khan, M. A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system. *Entropy* **2018**, *20*, 913. [CrossRef]
9. Munir, N.; Khan, M. A generalization of algebraic expression for nonlinear component of symmetric key algorithms of any characteristic p. In Proceedings of the 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 4–5 September 2018.
10. Liao, X.; Yu, Y.; Li, B.; Li, Z.; Qin, Z. A new payload partition strategy in color image steganography. *IEEE Trans. Circuits and Syst. Video Tech.* **2019**, *30*, 685–696. [CrossRef]
11. Liao, X.; Yin, J.; Guo, S.; Li, X.; Sangaiah, A.K. Medical JPEG image steganography based on preserving inter-block dependencies. *Comput. Electr. Eng.* **2018**, *67*, 320–329. [CrossRef]
12. Will, M.; William, B.; Jawad, A. An authentication protocol based on chaos and zero knowledge proof. *Nonlinear Dyn.* **2020**. [CrossRef]
13. Belkhouche, F.; Qidwai, U. Binary image encoding using 1D chaotic maps. In Proceedings of the Annual Technical Conference IEEE Region 5, New Orleans, LA, USA, 11 April 2003.
14. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractal* **2004**, *21*, 749–761. [CrossRef]
15. Habutsu, T.; Nishio, Y.; Sasase, I.; Mori, S. A secret key cryptosystem by iterating a chaotic map. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, 8–11 April 1991.
16. Liao, X.; Lai, S.; Zhou, Q. A novel image encryption algorithm based on self-adaptive wave transmission. *Signal Process.* **2010**, *90*, 2714–2722. [CrossRef]
17. Mao, Y.; Chen, G.; Lian, S. A novel fast image encryption scheme based on 3D chaotic baker maps. *Int. J. Bifurcation Chaos* **2004**, *14*, 3613–3624. [CrossRef]
18. Annaby, M.H.; Rushdi, M.A.; Nehary, E.A. Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion. *Opt. Lasers Eng.* **2018**, *103*, 9–23. [CrossRef]
19. Sun, F.; Liu, S.; Li, Z.; Lü, Z. A novel image encryption scheme based on spatial chaos map. *Chaos Solitons Fractals* **2008**, *38*, 631–640. [CrossRef]
20. Guo, J.I. A new chaotic key-based design for image encryption and decryption. In Proceedings of the 2000 IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, 28–31 May 2000.
21. Zhang, Q.; Guo, L.; Wei, X. Image encryption using DNA addition combining with chaotic maps. *Math. Comput. Mod.* **2010**, *52*, 2028–2035. [CrossRef]
22. Zhang, G.; Liu, Q. A novel image encryption method based on total shuffling scheme. *Opt. Commun.* **2011**, *284*, 2775–2780. [CrossRef]
23. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
24. Karmeshu, J. *Entropy Measures, Maximum Entropy Principle and Emerging Applications*, 2003 ed.; Springer: Berlin, Germany, 2003.
25. Khan, M.; Masood, F.; Alghafis, A.; Amin, M.; Batool Naqvi, S.I. A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion. *PLoS ONE* **2019**, *14*, e0225031. [CrossRef]
26. Behnia, S.; Akhshani, A.; Mahmodi, H.; Akhavan, A. A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos Solitons Fractals* **2008**, *35*, 408–419. [CrossRef]
27. Lian, S.; Sun, J.; Wang, Z. A block cipher based on a suitable use of the chaotic standard map. *Chaos Solitons Fractals* **2005**, *26*, 117–129. [CrossRef]
28. Wang, Y.; Wong, K.W.; Liao, X.; Chen, G. A new chaos-based fast image encryption algorithm. *Appl. Softw. Comput.* **2011**, *11*, 514–522. [CrossRef]
29. Wong, K.W.; Kwok, B.S.H.; Law, W.S. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A* **2008**, *372*, 2645–2652. [CrossRef]
30. Khan, M.; Masood, F.; Alghafis, A. Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system. *Neur. Comput. Appl.* **2019**, 1–21. [CrossRef]
31. Agarwal, S. Secure image transmission using fractal and 2D-chaotic map. *J. Imaging* **2018**, *4*, 17. [CrossRef]

32. Minas, N.A.; Mohammed Sediq, F.H.; Salih, A.I. Color Image Encryption Using Hybrid Method of Fractal-Based Key and Private XOR Key. *Kirkuk Univ. J. Sci. Stud.* **2018**, *13*, 104–117.
33. Gupta, S.; Bansal, N. Image encryption techniques using fractal geometry: A comparative study. *IOSR J. Comput. Eng.* **2014**, *16*, 31–35. [CrossRef]
34. Mandelbrot, B.B. *The Fractal Geometry of Nature*; Henry Holt and Company: New York, NY, USA, 1982.
35. Crownover, R.M. *Introduction to Fractals and Chaos*, 1st ed.; Jones & Bartlett Pub: Burlington, MA, USA, 1995.
36. Abd-El-Hafiz, S.K.; Radwan, A.G.; Haleem, S.H.A.; Barakat, M.L. A fractal-based image encryption system. *IET Image Process.* **2014**, *8*, 742–752. [CrossRef]
37. Motýl, I.; Jašek, R.O.M.A.N.; Vařacha, P.A.V.E.L. Analysis of the fractal structures for the infor2mation encrypting process. *Int. J. Comput.* **2012**, *4*, 224–231.
38. Kumar, S. Public key cryptographic system using Mandelbrot sets. In Proceedings of the MILCOM 2006-2006 IEEE Military Communications Conference, Washington, DC, USA, 23–25 October 2006.
39. Sun, Y.; Xu, R.; Chen, L.; Hu, X. Image compression and encryption scheme using fractal dictionary and Julia set. *IET Image Process* **2015**, *9*, 173–183. [CrossRef]
40. Mikhail, M.; Abouelseoud, Y.; ElKobrosy, G. Two-phase image encryption scheme based on FFCT and fractals. *Secur. Commun. Netw.* **2017**, *2017*, 1–13. [CrossRef]
41. Ahmad, J.; Larijani, H.; Emmanuel, R.; Mannion, M. Secure occupancy monitoring system for IoT using lightweight intertwining logistic map. In Proceedings of the 2018 10th Computer Science and Electronic Engineering (CEEC), Colchester, UK, 19–21 September 2018.
42. Ahmad, J.; Larijani, H.; Emmanuel, R.; Mannion, M.; Javed, A.; Ahmadinia, A. An intelligent real-time occupancy monitoring system with enhanced encryption and privacy. In Proceedings of the 2018 IEEE 17th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC), Berkeley, CA, USA, 16–18 July 2018.
43. Khan, J.S.; ur Rehman, A.; Ahmad, J.; Habib, Z. A new chaos-based secure image encryption scheme using multiple substitution boxes. In Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 18 December 2015.
44. Stallings, W. *Cryptography and Network Security*, 4th ed.; McGraw-Hill, Inc.: New York, NY, USA, 2007.
45. Matthews, R. On the derivation of a "chaotic" encryption algorithm. *Cryptologia* **1989**, *13*, 29–42. [CrossRef]
46. Baptista, M.S. Cryptography with chaos. *Phys. Lett. A* **1998**, *240*, 50–54. [CrossRef]
47. Hilborn, R.C. *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, 2nd ed.; Oxford University Press Inc.: New York, NY, USA, 2000.
48. Alexan, W.; Hamza, A.; Medhat, H. An aes double–layer based message security scheme. In Proceedings of the 2019 International Conference on Innovative Trends in Computer Engineering, Aswan, Egypt, 2–4 February 2019.
49. Elkandoz, M.T.; Alexan, W.; Hussein, H.H. 3D Image Steganography Using Sine Logistic Map and 2D Hyperchaotic Map. In Proceedings of the 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 19–21 November 2019.
50. Khan, M.; Munir, N. A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic. *Wirel. Per. Commun.* **2019**, *109*, 849–867. [CrossRef]
51. Ali, K.M.; Khan, M. Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. *Int. J. Theor. Phys.* **2019**, *58*, 3091–3117. [CrossRef]
52. Khan, M. A novel image encryption scheme based on multiple chaotic S-boxes. *Nonlinear Dyn.* **2015**, *82*, 527–533. [CrossRef]
53. Ahmad, J.; Hwang, S.O. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimed. Tools Appl.* **2016**, *75*, 13951–13976. [CrossRef]
54. Ahmad, J.; Hwang, S.O. Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dyn.* **2015**, *82*, 1839–1850. [CrossRef]
55. Ahmad, J.; Khan, M.A.; Hwang, S.O.; Khan, J.S. A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neur. Comput. Appl.* **2017**, *28*, 953–967. [CrossRef]
56. Norouzi, B.; Mirzakuchaki, S.; Seyedzadeh, S.M.; Mosavi, M.R. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimed. Tools Appl.* **2014**, *71*, 1469–1497. [CrossRef]

57. Ahmad, J.; Hwang, S.O.; Ali, A. An experimental comparison of chaotic and non-chaotic image encryption schemes. *Wirel. Per. Commun.* **2015**, *84*, 901–918. [CrossRef]
58. Batool, S.I.; Waseem, H.M. A novel image encryption scheme based on Arnold scrambling and Lucas series. *Multimed. Tools Appl.* **2019**, *78*, 1–27. [CrossRef]
59. Kumar, A.; Kar, M.; Mandal, M.K.; Nandi, D. Image encryption using four-dimensional hyper chaotic Lorenz system. *Elixir Elec. Eng.* **2016**, *87*, 41904–41909.
60. Shah, S.A.; Yang, X.; Abbasi, Q.H. Cognitive health care system and its application in pill-rolling assessment. *Int. J. Numer. Mod. Electr. Netw. Dev. Fields* **2019**, *32*, e2632. [CrossRef]
61. Shah, S.A.; Fioranelli, F. RF sensing technologies for assisted daily living in healthcare: A comprehensive review. *IEEE Aerosp. Electr. Syst. Mag.* **2019**, *34*, 26–44. [CrossRef]
62. Shah, S.A.; Fioranelli, F. Human Activity Recognition: Preliminary Results for Dataset Portability using FMCW Radar. In Proceedings of the 2019 International Radar Conference, Toulon, France, 23–27 September 2019.
63. Tahir, A.; Ahmad, J.; Shah, S.A.; Morison, G.; Skelton, D.A.; Larijani, H.; Abbasi, Q.H.; Imran, M.A.; Gibson, R.M. WiFreeze: Multiresolution scalograms for freezing of gait detection in Parkinson's leveraging 5G spectrum with deep learning. *Electronics* **2019**, *8*, 1433. [CrossRef]
64. Yang, X.; Fan, D.; Ren, A.; Zhao, N.; Shah, S.A.; Alomainy, A.; Ur-Rehman, M.; Abbasi, Q.H. Diagnosis of the Hypopnea syndrome in the early stage. *Neur. Comput. Appl.* **2020**, *32*, 855–866. [CrossRef]
65. Rani, M.; Kumar, V. Superior Julia set. *Res. Math. Edu.* **2004**, *8*, 261–277.
66. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
67. Mazloom, S.; Eftekhari-Moghadam, A.M. Color image encryption based on coupled nonlinear chaotic map. *Chaos Solitons Fractals* **2009**, *42*, 1745–1754. [CrossRef]
68. Seyedzadeh, S.M.; Mirzakuchaki, S. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal Process.* **2012**, *92*, 1202–1215. [CrossRef]
69. Liu, S.; Sun, J.; Xu, Z. An Improved Image Encryption Algorithm based on Chaotic System. *Jcp* **2009**, *4*, 1091–1100. [CrossRef]
70. Akhshani, A.; Akhavan, A.; Lim, S.C.; Hassan, Z. An image encryption scheme based on quantum logistic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 4653–4661. [CrossRef]
71. Wang, X.; Teng, L.; Qin, X. A novel color image encryption algorithm based on chaos. *Signal Process.* **2012**, *92*, 1101–1108. [CrossRef]
72. El-Latif, A.A.A.; Li, L.; Wang, N.; Han, Q.; Niu, X. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process.* **2013**, *93*, 2986–3000. [CrossRef]
73. Wang, X.; Yang, L. A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models. *Opt. Commun.* **2012**, *285*, 4033–4042. [CrossRef]
74. Wu, Y.; Zhou, Y.; Noonan, J.P.; Agaian, S. Design of image cipher using latin squares. *Inf. Sci.* **2014**, *264*, 317–339. [CrossRef]
75. Khan, M.; Shah, T. An efficient chaotic image encryption scheme. *Neur. Comput. Appl.* **2015**, *26*, 1137–1148. [CrossRef]
76. Huang, C.K.; Nien, H.H. Multi chaotic systems-based pixel shuffle for image encryption. *Opt. Commun.* **2009**, *282*, 2123–2127. [CrossRef]
77. Rhouma, R.; Meherzi, S.; Belghith, S. OCML-based colour image encryption. *Chaos Soliton Fractals* **2009**, *40*, 309–318. [CrossRef]
78. Gupta, K.; Silakari, S. Novel approach for fast compressed hybrid color image cryptosystem. *Adv. Eng. Softw.* **2012**, *49*, 29–42. [CrossRef]
79. Kadir, A.; Hamdulla, A.; Guo, W. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik* **2014**, *125*, 1671–1675. [CrossRef]
80. Liu, H.; Wang, X.; Kadir, A. Image encryption using DNA complementary rule and chaotic maps. *Appl. Softw. Comput.* **2012**, *12*, 1457–1466. [CrossRef]
81. Wei, X.; Guo, L.; Zhang, Q.; Zhang, J.; Lian, S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *J. Syst. Softw.* **2012**, *85*, 290–299. [CrossRef]
82. Liu, L.; Zhang, Q.; Wei, X. A RGB image encryption algorithm based on DNA encoding and chaos map. *Comput. Electr. Eng.* **2012**, *38*, 1240–1248. [CrossRef]
83. Belazi, A.; El-Latif, A.A.A.; Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* **2016**, *128*, 155–170. [CrossRef]

84. Hamza, R.; Titouna, F. A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. *Inf. Secur. J. A Glob. Perspect.* **2016**, *25*, 162–179. [CrossRef]
85. Huang, X.; Ye, G. An image encryption algorithm based on hyper-chaos and DNA sequence. *Multimed. Tools Appl.* **2014**, *72*, 57–70. [CrossRef]
86. Wang, X.; Liu, L.; Zhang, Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Opt. Lasers Eng.* **2015**, *66*, 10–18. [CrossRef]
87. Khan, M.; Asghar, Z. A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation. *Neur. Comput. Appl.* **2018**, *29*, 993–999. [CrossRef]
88. Wang, X.Y.; Zhang, Y.Q.; Bao, X.M. A colour image encryption scheme using permutation-substitution based on chaos. *Entropy* **2015**, *17*, 3877–3897. [CrossRef]
89. Machkour, M.; Saaidi, A.; Benmaati, M.L. A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher. *3D Res.* **2015**, *6*, 36. [CrossRef]
90. Ahmed, F.; Anees, A.; Abbas, V.U.; Siyal, M.Y. A noisy channel tolerant image encryption scheme. *Wirel. Per. Commun.* **2014**, *77*, 2771–2791. [CrossRef]