symmetry

MDPI

Article

RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System †

Wassim Alexan [1,*], **Mohamed ElBeltagy** [1] and **Amr Aboshousha** [2]

[1] Faculty of IET, The German University in Cairo, Cairo 11835, Egypt; mohamed.elbeltagy@ieee.org
[2] The Physics Department, The German University in Cairo, Cairo 11835, Egypt; amr.aboshousha@guc.edu.eg
* Correspondence: wassim.joseph@guc.edu.eg

† This journal paper is an extension of the authors' previous conference paper: Alexan, W.; ElBeltagy, M.; Aboshousha, A. Lightweight Image Encryption: Cellular Automata and the Lorenz System. In Proceedings of the 2021 International Conference on Microelectronics (ICM), Cairo, Egypt, 19–22 December 2021; pp. 34–39. https://doi.org/10.1109/ICM52667.2021.9664961.

Abstract: The exponential growth in transmission of multimedia over the Internet and unsecured channels of communications is putting pressure on scientists and engineers to develop effective and efficient security schemes. In this paper, an image encryption scheme is proposed to help solve such a problem. The proposed scheme is implemented over three stages. The first stage makes use of Rule 30 cellular automata to generate the first encryption key. The second stage utilizes a well-tested S-box, whose design involves a transformation, modular inverses, and permutation. Finally, the third stage employs a solution of the Lorenz system to generate the second encryption key. The aggregate effect of this 3-stage process insures the application of Shannon's confusion and diffusion properties of a cryptographic system and enhances the security and robustness of the resulting encrypted images. Specifically, the use of the PRNG bitstreams from both of the cellular automata and the Lorenz system, as keys, combined with the S-box, results in the needed non-linearity and complexity inherent in well-encrypted images, which is sufficient to frustrate attackers. Performance evaluation is carried out with statistical and sensitivity analyses, to check for and demonstrate the security and robustness of the proposed scheme. On testing the resulting encrypted Lena image, the proposed scheme results in an MSE value of 8923.03, a PSNR value of 8.625 dB, an information entropy of 7.999, NPCR value of 99.627, and UACI value of 33.46. The proposed scheme is shown to encrypt images at an average rate of 0.61 Mbps. A comparative study with counterpart image encryption schemes from the literature is also presented to showcase the superior performance of the proposed scheme.

Keywords: image encryption; cellular automata; S-box; Lorenz system; NIST analysis

check for updates

Citation: Alexan, W.; ElBeltagy, M.; Aboshousha, A. RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System. *Symmetry* **2022**, *14*, 443. https://doi.org/10.3390/sym14030443

Academic Editors: Debiao He and Manuel Manas

Received: 30 November 2021
Accepted: 21 February 2022
Published: 23 February 2022

1. Introduction

The unprecedented developments and complexity witnessed in today's wireless communication networks and big data applications render security as an issue of paramount importance [1–3]. Data security, through cryptography and steganography [4–9], has thus become a vital means to ensure safe and secure operation and usage of millions of online applications [10]. Cryptography, being the core technology in information security, has attracted the attention of scientists and engineers, with investments in its research and developments skyrocketing in recent decades [11,12]. Although modern cryptographic algorithms employ block ciphers such as the data encryption standard (DES), the triple DES (3DES), and the advanced encryption standard (AES), they are not best-suited for the purposes of encrypting images. This is because images hold very large amounts of data [13]. Thus, global efforts in recent years were directed to design and build cryptosystems that are lightweight and better-suited to efficiently carry out image encryption. Outcomes of such efforts have usually involved the use of one or more pseudo random number generators (PRNGs) as well as true RNGs. The literature includes examples pooling from chaos theory [14], cellular automata (CA) [15], electrical circuits [16] and electronics [17], quantum physics [18], as well as many others. The next few paragraphs emphasize the importance of CA and chaos theory in security applications, as well as their utilization in state-of-the-art image encryption schemes. Next, substitution boxes (S-boxes) are discussed as a powerful tool to introduce confusion in a cryptosystem.

Cellular automata are systems of dynamical nature that are discrete both in space and time. A cellular automaton comprises an array of cells. Each such cell can take on a value from a finite number of possibilities, updated synchronously in discrete steps of time, based on an interaction rule. As many cryptographic algorithms are based on RNGs, CA seems to be a great fit, as they can be utilized as RNGs with multiple advantages. Those include algorithmic simplicity and the ease of hardware implementation [19]. One of the earliest uses of CA in cryptography was proposed by Wolfram in [20]. Soon enough, scientists and engineers adopted the idea of CA as encryption devices and started utilizing them as well. Most notably is the work of Nandi et al. [21], where a number of block and stream ciphers were proposed. These were based on CA built around Rule 51, Rule 90, Rule 150, Rule 153, and Rule 195. Achieved numerical results clearly showcase that the use of CA provides good defense against various attacks. Furthermore, the authors of [21] also proposed logic diagrams for VLSI implementations of such CA based encryption hardware. A more recent work entailing the use of Rule 30 is [22], where the authors contend that because randomly generated numbers from Rule 30 are tested for significant randomness, it can be applied in visual cryptography schemes with much success. In [23], the authors propose an image encryption algorithm that utilizes a memrestive hyperchaotic system, CA, and DNA sequence operations. Furthermore, they make use of SHA-256 in their key generation. The authors of [24] adopted a non-uniform CA framework to circumvent the problem of the limited number of CA reversal rules and the inability to generate long state sequences by some of them. In [25], the authors present an image encryption scheme built on a quantum logistic map, CA, and an RSA-based key generation. The authors of [26] employ a multi-delay Chebyshev map, along with CA and DNA coding for the purposes of image encryption. The work proposed by [27] also employs chaos theory in addition to CA, as well as adopts SHA-2. To date, the amount of literature making use of CA in cryptography is rather limited, especially when compared to its equivalent amount that extends ideas from chaotic and dynamical systems for the same purposes of security.

The inherent characteristics of chaotic functions as a random phenomenon in nonlinear systems prove advantageous in relation to cryptography [14], specifically, their high sensitivity to initial conditions, control parameters, periodicity, pseudo-randomness, and ergodicity [28]. These characteristics are made use of in designing image encryption schemes. Such schemes are classified into two categories: (a) one-dimensional (1D) and (b) multi-dimensional (MD). Although image encryption schemes that are based on 1D chaotic maps are less complex and more efficient for software and hardware implementations, they exhibit less desirable characteristics, in terms of shorter chaotic periods, non-uniform distribution of their chaotic output, and a higher vulnerability to cryptanalysis. In contrast, MD chaotic maps when employed in image encryption schemes provide higher security levels at the expense of a higher complexity and, thus, more running time for software and hardware implementations [29]. The literature on the use of 1D and MD for image encryption is extensive. For example, the authors of [30] propose a grayscale image encryption algorithm based on pixel shuffling through the Arnold map, followed by the use of a key that is generated through the 2D logistic sine map and a linear congruential generator. The authors of [31] utilized a finite field in order to generalize the logistic map and attempt to find an automorphic mapping between two logistic maps to compute parameters over the finite field Z_N. In [32], the authors employ a coupling of the 2D logistic map and a quantum chaotic map through the nearest-neighboring coupled-map matrices. Their proposed scheme makes use of the resulting higher complexity randomness to generate an encrypted image. The authors of [33] propose a symmetric cryptosystem for color images. Their proposed algorithm employs a hybrid form of the Lorenz system to achieve diffusion and DNA sequencing to achieve confusion. In [34], the authors make use of a Lorenz–Rossler chaotic system to carry out pixel diffusion, whereas 2D logistic maps are employed for confusion. The authors of [35] propose a color image encryption scheme that utilizes multiple chaotic maps with a minimum number of rounds of encryption. Their proposed scheme makes full use of the ideas of Shannon with regards to confusion and diffusion. A rather thorough numerical analysis was carried out by the authors of [36], who proposed a scheme based on an LA-semi group for confusion, whereas a chaotic continuous system was adopted for diffusion. In [37], the authors base their proposed image encryption scheme on three stages: A diffusion stage that utilizes a chaotic quantum logistic function, a scrambling stage for the pixel arrangement, which employs a 2D chaotic map, and then coupling the results of the first two stages with a nearest-neighbor coupled-map lattices. The authors of [38] propose an efficient image encryption scheme that is based on hyper-chaos and a vector operation. Their proposed scheme makes use of a post-processing method that creates a key matrix. The use of this key matrix results in an acute reduction in the number of required iterations of the utilized hyperchaotic system. In [39], a color image encryption scheme that involves the use of chaos theory and a zigzag transform is proposed. The authors employ the zigzag transform in conjunction with an arrangement that changes in a bidirectional crossover manner to carry out the first stage of image encryption. This is followed by the use of a logistic map and a hyperchaotic Chen dynamical system. This paragraph only touches upon the topic of employing chaos theory in image encryption applications. Recent literature on the topic is quite expansive. The next paragraph focuses on a different but rather important building block of many image encryption schemes: substitution boxes.

An S-box is a vital component in modern block encryption algorithms. It aids in generating an apparent ciphertext from any given plaintext. The simple act of adding an S-box to an encryption algorithm results in a non-linear mapping between the input and output data, thus providing the confusion property [40]. The higher the extent of confusion, the better the security offered by an S-box in a block cipher. In turn, for many block encryption algorithms, their robustness against attacks is directly related to the security provided through the utilization of one or more S-boxes. Although such algorithms could comprise multiple components, an S-box is usually the sole non-linear component that enhances sensitive data security [41,42]. State-of-the-art symmetric ciphers usually employ S-boxes that introduce a high level of confusion for attackers [13,43–46]. However, designing an S-box should be an efficient and low-complexity process in order for it to be suitable for real-time data encryption algorithms. For example, the generation of S-boxes through the employment of a linear fractional transformation (LFT) makes use of the Galois field. LFT, otherwise known as the Möbius transformation, is repeatedly mentioned in the literature for the design of S-boxes [47,48].

While recent literature on image encryption schemes proposes a multitude of algorithms that make use of chaos theory, very little research utilizes CA. Furthermore, the combined utilization of chaos theory and CA for image encryption is very limited in the literature. Schemes that do propose such combinations either suffer from low key spaces or lengthy encryption times, deeming them less than optimal for modern-day real-time image encryption applications. In this paper, the authors identify this as a research gap and attempt to fill it, by proposing a novel color image encryption scheme that combines ideas from chaos theory and CA. Furthermore, the proposed scheme possesses a large key space, yet exhibits a very small encryption time. The contributions of this paper are as follows. A lightweight color image encryption scheme is proposed. The proposed scheme is based on three stages. The first stage incorporates the use of Rule 30 CA, the second stage utilizes a robust S-box, and the third stage employs a solution of the Lorenz system. The proposed image encryption scheme makes use of the ideas of confusion and diffusion proposed by Shannon [49]. Performance analysis is carried out and compared against recent counterpart image encryption schemes from the literature. The computed numerical results are remarkable in terms of robustness and resistance to statistical and differential attacks. The proposed scheme is also shown to pass the NIST suite of tests. Finally, its suitability for real-time applications is evaluated, given its large key space and short running time. This paper is organized as follows. Section 2 introduces some preliminary ideas that are employed in the proposed scheme. Those include Rule 30 of CA, followed by the adopted S-box and the Lorenz system. Section 3 describes the methodology of the proposed image encryption scheme. Section 4 presents the numerical results of the computations and performance evaluation and provides appropriate commentary on them. Section 5 draws the conclusions of the paper, identifies a limitation, and suggests future work that could be further pursued.

2. Preliminary for the Proposed Image Encryption Scheme

The proposed image encryption scheme is composed of three stages. The first stage involves the use of Rule 30 cellular automaton to generate the first encryption key. The second stage makes use of an S-box. Finally, the third stage employs a solution of the Lorenz system to generate a second encryption key. The next sections introduce each of those concepts.

2.1. Rule 30 Cellular Automaton

A simple 2D cellular automaton is basically a 2D array with each cell taking 1 of 2 values, in this case, a 0 (white) or a 1 (black), plotted on an infinite sheet of graph paper, with a set of rules defining how the next cells would take on values. The neighborhood of a cell is defined in one of the two following ways: (1) The von Neumann neighborhood, and (2) The Moore neighborhood [50]. Figure 1 shows each of the neighborhoods of the center cell in each of the cellular automata. However, for the purposes of the image encryption scheme proposed in this paper, we are only interested in the simplest nontrivial cellular automaton with a cell's neighborhood defined as the adjacent cells on either side of it. Thus, for any any given cell, along with its two neighbors, it would form a neighborhood of three cells, resulting in $2^3 = 8$ possible patterns. Rule 30 cellular automaton exhibits a class 3 behavior. This means that simple input patterns lead to chaotic and rather random outputs. Mathematically, Rule 30 gives the next state of any given cell as

$$s_i(t+1) = s_{i-1}(t) \oplus (s_i(t) + s_{i+1}(t)), \tag{1}$$

where $\oplus$ and $+$ on the RHS of (1) are the "xor" and "or" Boolean operators, respectively.

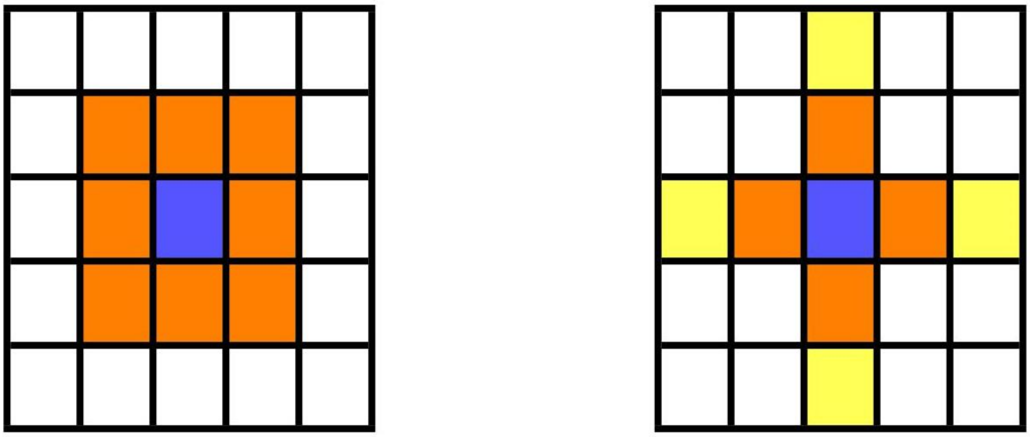


Figure 1. The orange cells are the Moore neighborhood for the violet cell (**left**). The orange cells are the von Neumann neighborhood for the violet cell. The range-2 cross neighborhood includes the yellow cells also (**right**).

Figure 2 shows the utilization of the pattern shown in Figure 3 and expressed mathematically in (1) to generate the first 10 steps of the Rule 30 cellular automaton. Starting with the top row, there is only a single black cell, having a value of 1. This means that both of its adjacent neighbors are white cells, having a value of 0. Referring back to Figure 3, the sixth square depicts the current situation and shows a next cell that is also black, having a value of 1. Repeated utilization of the pattern in Figure 3 results in the generation of Figure 2 for 10 steps and Figure 4 for 100 steps. It was suggested in [15] that Rule 30 cellular automaton can be considered as a PRNG, as the center column satisfies the characteristics of a randomly generated bitstream. For example, examining the center column of Figure 2 reveals that the resulting bitstream is $\{1,1,0,1,1,1,0,0,1,1,0\}$. Based on the work of Wolfram in [20], this fact was first utilized in [51] for the introduction of a block cipher for use in public-key cryptography. This is because given the rule, it is a straight forward process to compute future states; however, it is rather complex to compute previous ones.

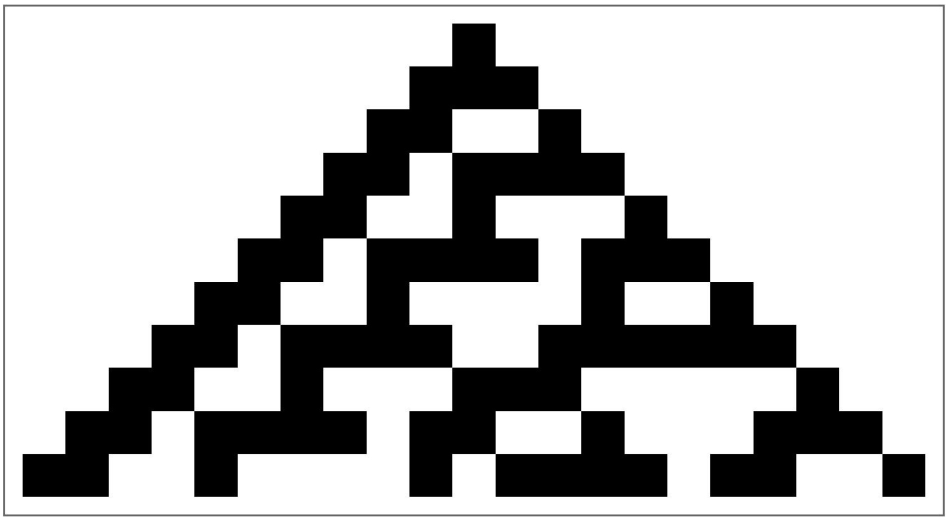


Figure 2. The first 10 steps of Rule 30 cellular automaton.

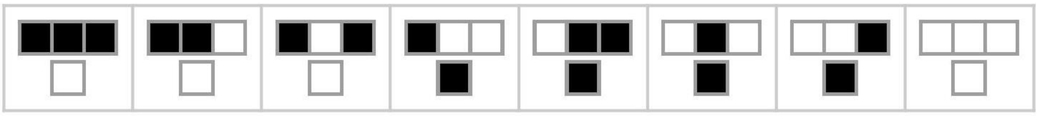


Figure 3. Current pattern and new state for center cell of a Rule 30 cellular automaton.

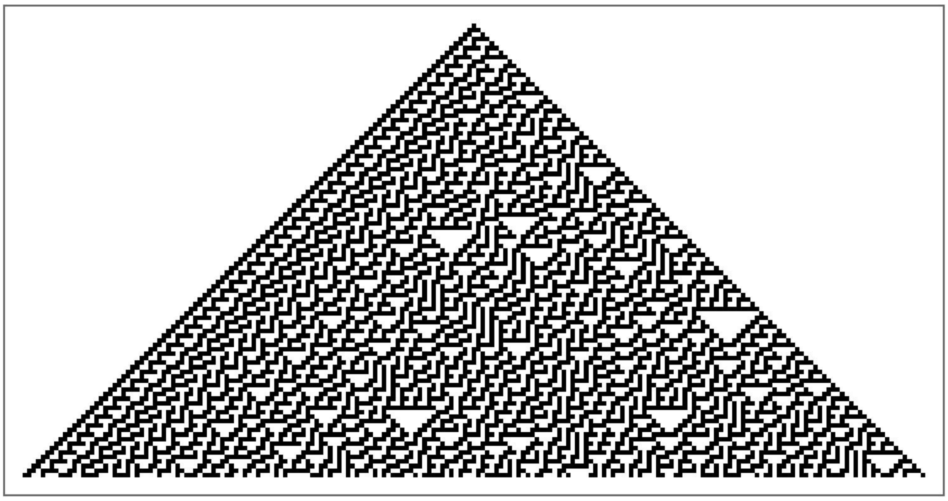


Figure 4. The first 100 steps of Rule 30 cellular automaton.

2.2. S-Box

With the security and robustness of block ciphers being heavily dependent on the cryptographic abilities of the utilized S-boxes to introduce adequate confusion effects, it becomes clear that the choice of an S-box should be of prime importance when attempting to design a robust and secure image encryption scheme. The authors of [43] also realize the importance of how S-boxes introduce non-linearity and complexity into a cryptosystem and thus propose a novel method for the construction of S-boxes. In their paper, they propose a modular approach that comprises three operations: a transformation, modular inverses, and a permutation. Following their approach, highly non-linear S-boxes can be efficiently generated, each through a simple change in the initial transformation parameters. In their paper, the authors of [43] subject one such example constructed S-box to a number of performance evaluation benchmarks. Those include testing for high non-linearity, absence of fixed points, possession of SAC and BIC characteristics, as well as low differential uniformity and linear approximation probability. Table 1 provides an example of an S-box generated using the ideas proposed in [43], which we employ in our proposed image encryption scheme.

Table 1. Example S-box values as constructed from the proposed method in [43].

203	153	138	245	187	130	186	167	144	40	131	250	202	47	244	136
141	166	91	116	121	13	210	55	7	126	217	113	90	71	127	70
12	119	104	54	190	88	184	32	42	248	112	158	89	11	209	154
229	30	207	220	195	23	216	128	118	102	109	255	249	4	53	1
211	74	197	206	235	198	18	193	81	149	19	117	115	31	5	147
231	25	182	242	163	14	177	180	254	24	208	123	111	84	224	178
161	201	157	133	175	236	218	241	106	165	137	213	36	162	38	230
10	205	107	69	97	251	159	222	191	65	57	93	179	212	17	72
76	20	214	194	61	125	114	101	34	152	171	122	228	68	85	199
170	83	0	174	87	58	172	189	29	135	86	105	223	156	143	132
196	63	43	237	181	185	240	45	78	164	200	192	66	35	98	6
160	188	150	52	247	27	219	95	221	44	120	92	151	16	39	21
82	124	100	56	96	79	33	173	146	134	49	233	3	77	80	243
94	15	75	232	26	110	252	226	142	140	238	108	176	64	239	59
22	51	60	183	46	67	204	253	8	2	148	155	139	129	41	234
62	37	50	227	28	103	48	246	168	99	145	9	215	225	73	169

2.3. The Lorenz System

A mathematical model for atmospheric convection was developed in 1963 by Edward Lorenz [52]. This model consists of three ordinary differential equations, now known as the Lorenz system. These differential equations are expressed as

$$\frac{dx}{dt} = \sigma(y - x), \tag{2a}$$

$$\frac{dy}{dt} = x(\rho - z) - y, \tag{2b}$$

$$\frac{dz}{dt} = xy - \beta z, \tag{2c}$$

where σ, ρ, and β are system parameters proportional to the Prandtl number, the Rayleigh number, and specific physical dimensions of the layer itself, respectively [53]. For the values $\sigma = 10, \beta = 8/3$, and $\rho = 28$, the system exhibits a chaotic behavior and its solution would be plotted as in Figure 5. This renders the Lorenz system to be a non-linear, non-periodic, 3D, and deterministic one. From a cryptographic point of view, the ability to generate a chaotic solution in a deterministic manner is highly appreciated [14], which is why we adopt it as part of our proposed image encryption scheme.

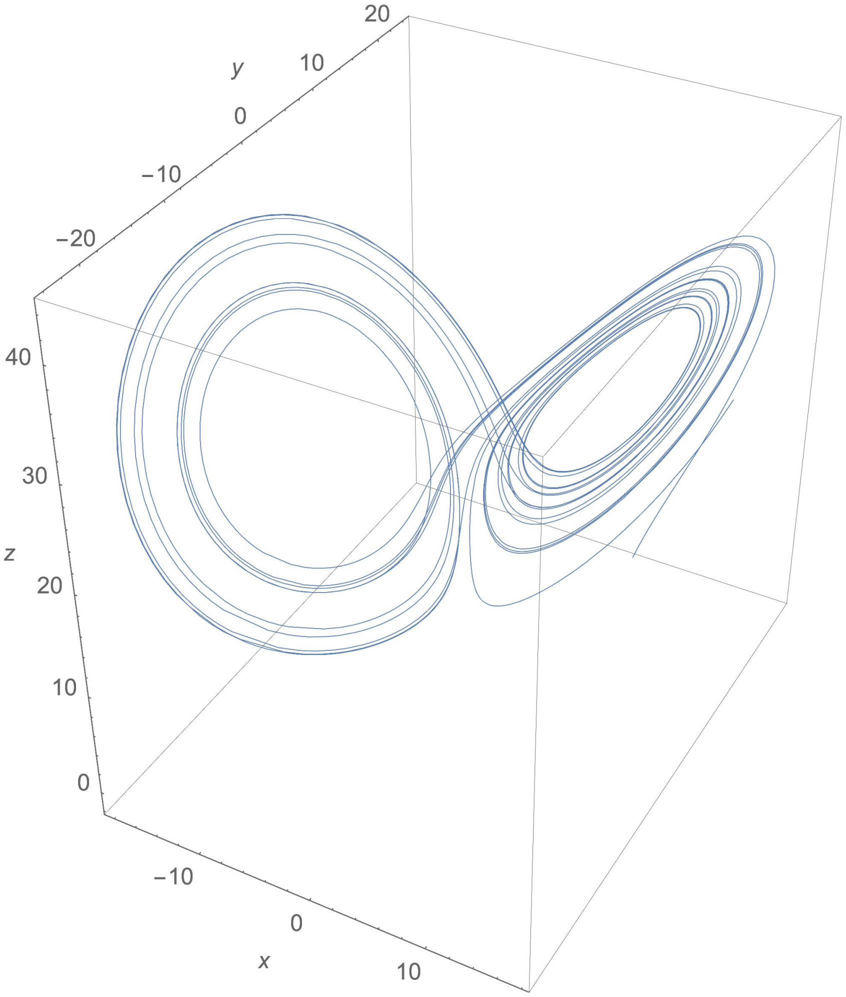


Figure 5. The butterfly shape of a Lorenz system solution for the values $\sigma = 10$, $\beta = 8/3$, and $\rho = 28$.

3. Methodology of the Proposed RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System

3.1. The Encryption Scheme

The proposed image encryption scheme is implemented in a number of steps, as follows.

1. An image of appropriate dimensions $M \times N$ is chosen and its pixels are converted into a 1D bitstream, d.
2. The mean intensity of the image pixels, P_μ, is calculated as

$$P_\mu = \frac{\sum_i p_i}{M \times N}, \tag{3}$$

where p_i is the intensity of pixel i. The resulting value is a rather small number, which we multiply by a magnifying factor f_M. Let us denote the resulting value by μ:

$$\mu = f_M \times P_\mu. \tag{4}$$

3. Cyclically shifting each of the a_i elements of d to the right by μ places:

$$\begin{tikzcd} a_0 \arrow[r] & a_1 \arrow[r] & a_2 \arrow[r] & \cdots \arrow[r] & a_k \arrow[llll, bend right] \end{tikzcd} \tag{5}$$

4. XORing the resulting bitstream, now denoted d_μ, with the first encryption key, K_{CA}, as follows:
$$C_0 = d_\mu \oplus K_{CA}, \tag{6}$$
where K_{CA} is a bitstream of the same length as d and d_μ, which is made up of a repetition of the first N_{CA} bits resulting from the center column of the Rule 30 CA as in Figure 6. This concludes the first stage of encryption.
5. The output bitstream from the XORing process, C_0, enters a substitution process using the proposed S-box, which is constructed employing the ideas proposed in [43]. Let us denote the resulting bitstream as C_1:
$$C_1 = S(C_0). \tag{7}$$
This concludes the second stage of encryption.
6. The Lorenz system is numerically solved, resulting in a 3D geometry, as depicted in Figure 5. Take the x, y, and z coordinates of each of the points of the resulting solution and flatten them into a single 1D array, L, as follows:
$$L = \{P_1, P_2, \ldots, P_M\} \rightarrow \{x_1, y_1, z_1, x_2, y_2, z_2, \ldots, x_M, y_M, z_M\}. \tag{8}$$
Next, we list plot those values into 2D, as shown in Figure 7. Examining the plot in Figure 7, it is clear that there are more positive values than there are negative ones. Therefore, we choose a threshold value λ, such that if any of the values are above this threshold, they would be accounted as 1s, otherwise, they would be accounted as 0 s, as follows:
$$v = \begin{cases} 1, & L_i > \lambda, \\ 0, & L_i \leq \lambda. \end{cases} \tag{9}$$
This newly obtained bitstream, v, of length N_L would make up the seed of our Lorenz system based key, as in Figure 8.
7. Repeat those N_L bits until they are of the same length as d and C_1, thus forming the second encryption key. Let us denote it K_L, and XOR it with C_1, obtaining C_2 as follows:
$$C_2 = C_1 \oplus K_L, \tag{10}$$
This concludes the third stage of encryption.
8. C_2 is reshaped back into an image of the same dimensions ($M \times N$) as those of the plain image, obtaining the encrypted image.

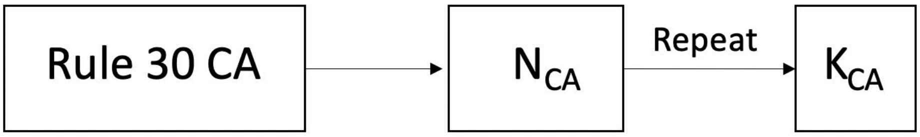


Figure 6. Flow chart of PRNG of Rule 30 CA, employed in the generation of the first key, K_{CA}.

Figure 9 provides a graphical illustration of the proposed image encryption scheme, and Figures 6 and 8 showcase the flow charts for the Rule 30 CA and the Lorenz system keys generation, respectively.

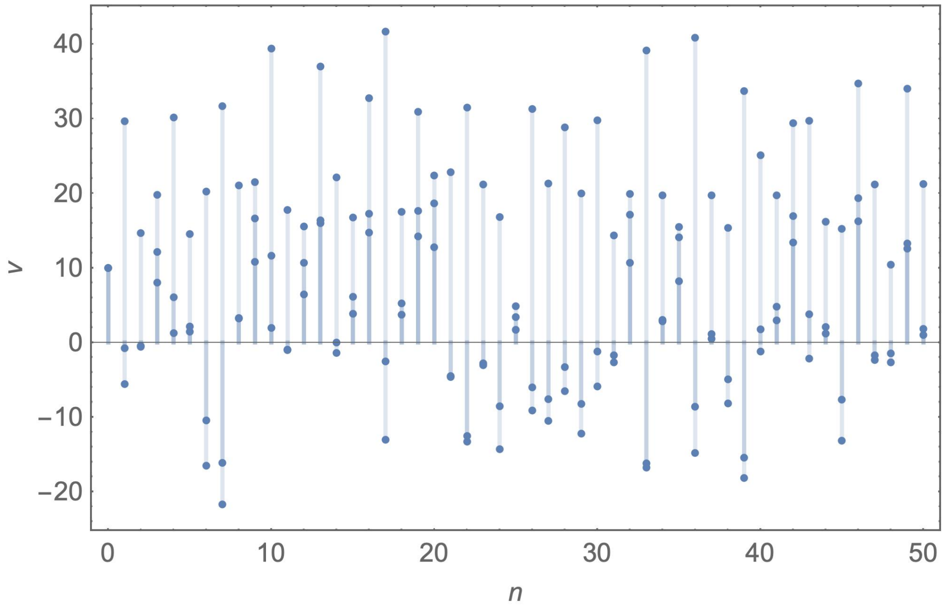
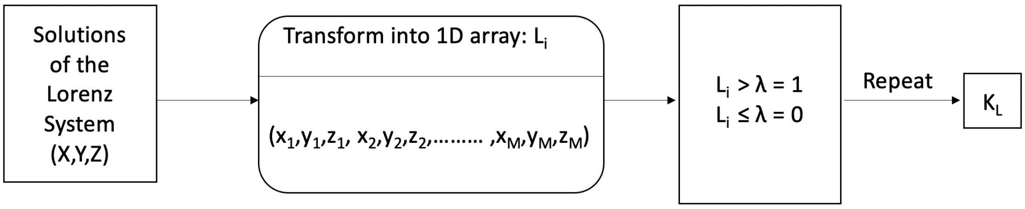


Figure 7. The first 50 points from the 2D array obtained from the 3D coordinates of the Lorenz system solution for the values $\sigma = 10, \beta = 8/3$, and $\rho = 28$.



Solutions of the Lorenz System (X,Y,Z)
Transform into 1D array: L_i
$(x_1,y_1,z_1, x_2,y_2,z_2,........ ,x_M,y_M,z_M)$
$L_i > \lambda = 1$
$L_i \leq \lambda = 0$
Repeat
K_L

Figure 8. Flow chart of PRNG of chaotic sequences from the Lorenz system, employed in the generation of the second key, K_L.

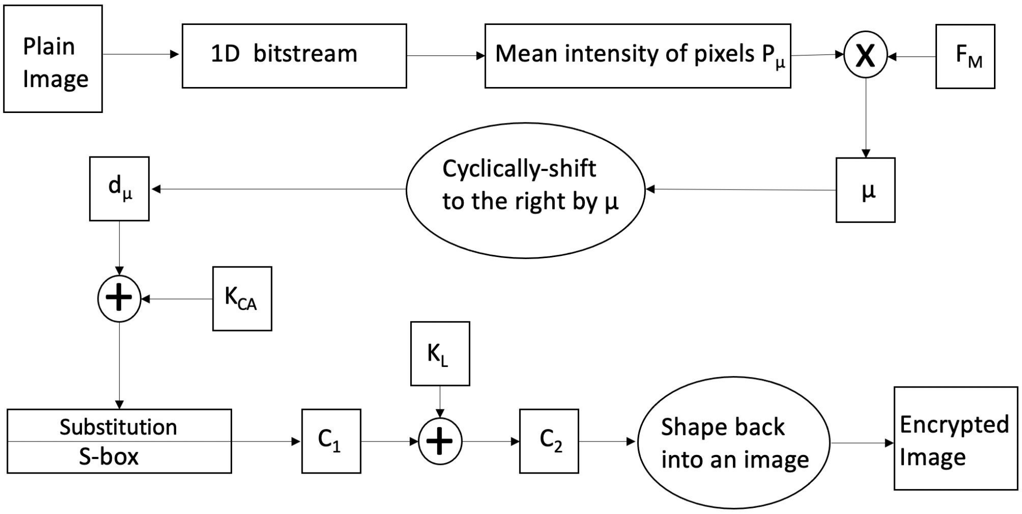


Figure 9. Flow chart of the encryption scheme.

3.2. The Decryption Scheme

The decryption scheme is implemented in a reverse manner as to that of the encryption scheme, in a number of steps as follows.

1. Grouping the bits of the encrypted image of dimensions $(M \times N)$ into a 1D bitstream, C_2.

2. XORing C_2 with the second encryption key, K_L, as follows:

$$C_1 = C_2 \oplus K_L \tag{11}$$

This concludes the first stage of decryption.

3. Applying an inverse substitution step on C_1, utilizing our generated S-box, as follows:

$$C_0 = S^{-1}(C_1) \tag{12}$$

This concludes the second stage of decryption.

4. Obtaining d_μ by XORing C_0 with the first encryption key, K_{CA}, as follows:

$$d_\mu = C_0 \oplus K_{CA} \tag{13}$$

This concludes the third stage of decryption.

5. Cyclically shifting each of the a_i bits of d_μ in the opposite direction to that used in the encryption, i.e., to the left, by the value of μ, resulting in a bitstream d

$$\begin{tikzcd} a_0 \arrow[rrrr, bend left] & a_1 \arrow[l] & a_2 \arrow[l] & \cdots \arrow[l] & a_k \arrow[l] \end{tikzcd} \qquad (14)$$

6. Folding back the resulting bitstream, d, into an image of the same dimensions ($M \times N$) as those of the encrypted image, obtaining the plain image.

Figure 10 provides a graphical illustration of the proposed image decryption scheme.

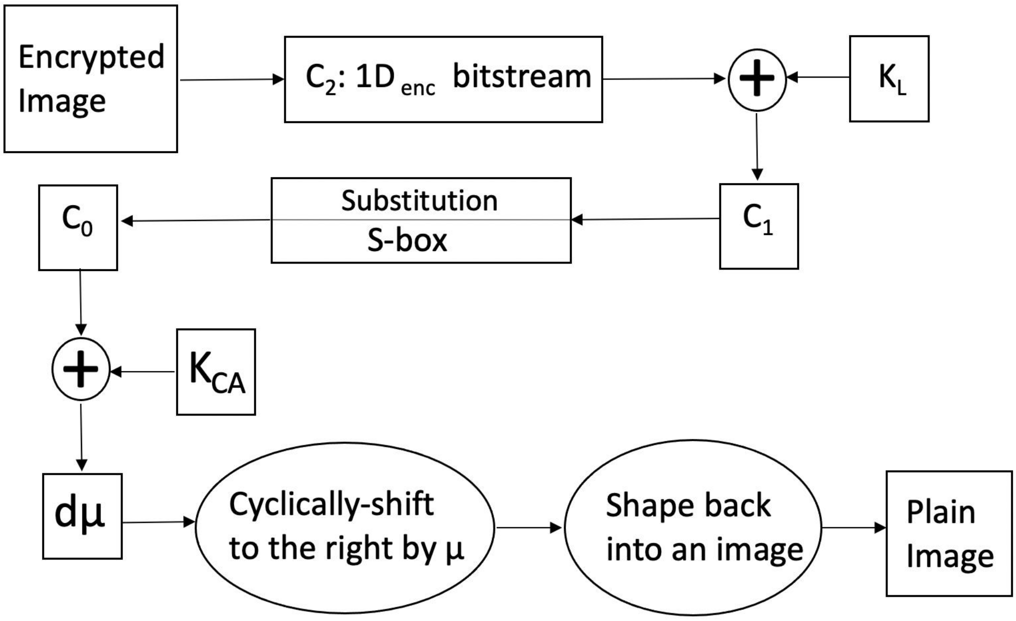


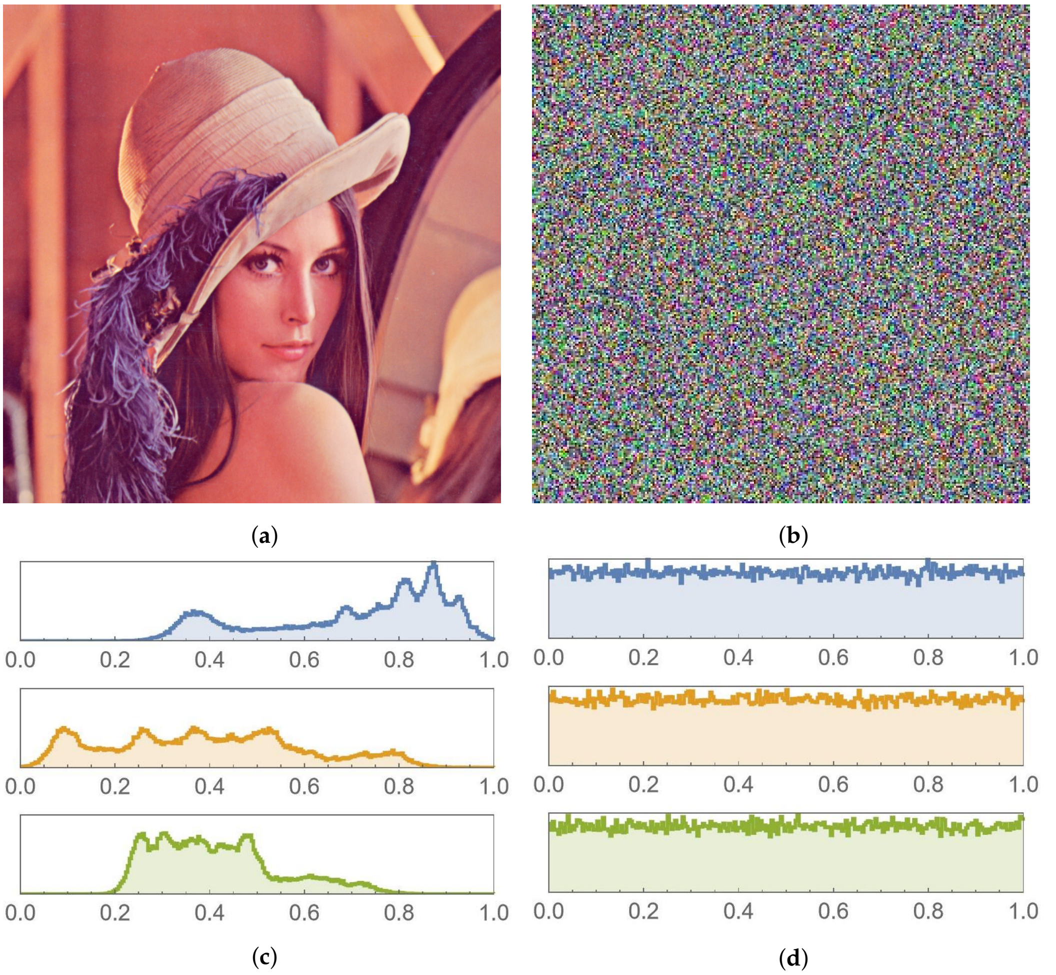
Figure 10. Flow chart of the decryption scheme.

4. Security Analysis and Numerical Results

The performance of an encryption algorithm is measured by its ability to resist statistical and differential attacks. Thus, this section outlines the numerical results of the proposed image encryption scheme, as well a comparison with its counterpart schemes from the literature. The proposed scheme is implemented using the computer algebra system Wolfram Mathematica® on a machine running macOS Catalina v10.15.7, equipped with a 2.9 GHz 6-Core Intel® Core$^{\mathrm{TM}}$ i9 processor and 32 GB of 2400 MHz DDR4 of memory. The utilized keys are assigned the following values: $\sigma = 10, \beta = 8/3, \rho = 28, N_{CA} = 100, N_L = 50, f_M = 10^6$, and $\lambda = 10$. Three images that are commonly used in image processing applications and experimentation are utilized in this section. These are Lena, Peppers, and Baboon, all of dimensions $M \times N = 256 \times 256$. The proposed image encryption scheme is tested against various statistical and differential attacks. Those include visual and histogram analyses, a correlation coefficient analysis, mean square error (MSE), mean absolute error (MAE), peak signal to noise ratio (PSNR), information entropy, a differential attack analysis, comprising the number of pixel changing rate (NPCR) and the unified average change intensity (UACI), a key space analysis, a NIST analysis, and, finally, an execution time analysis.

4.1. Visual and Histogram Analyses

The various sub-figures of Figures 11–13 depict plain and encrypted images of Lena, Peppers, and Baboon, respectively. It is clear that the human visual system (HVS) does not allow for any meaningful information to be discerned from the encrypted images.

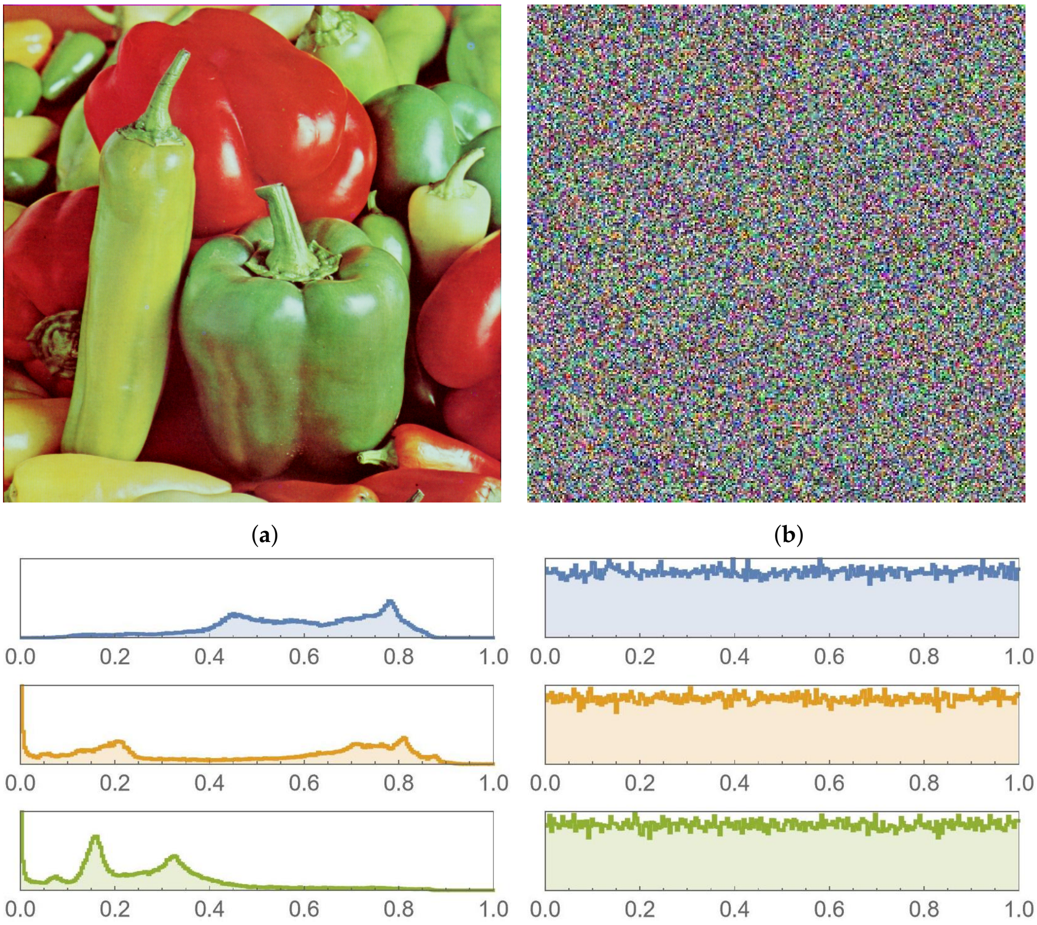


(**a**) (**b**)

(**c**) (**d**)

Figure 11. Lena image and histogram comparison before and after encryption. (**a**) Plain image. (**b**) Encrypted image. (**c**) Histogram of the plain image. (**d**) Histogram of the encrypted image.

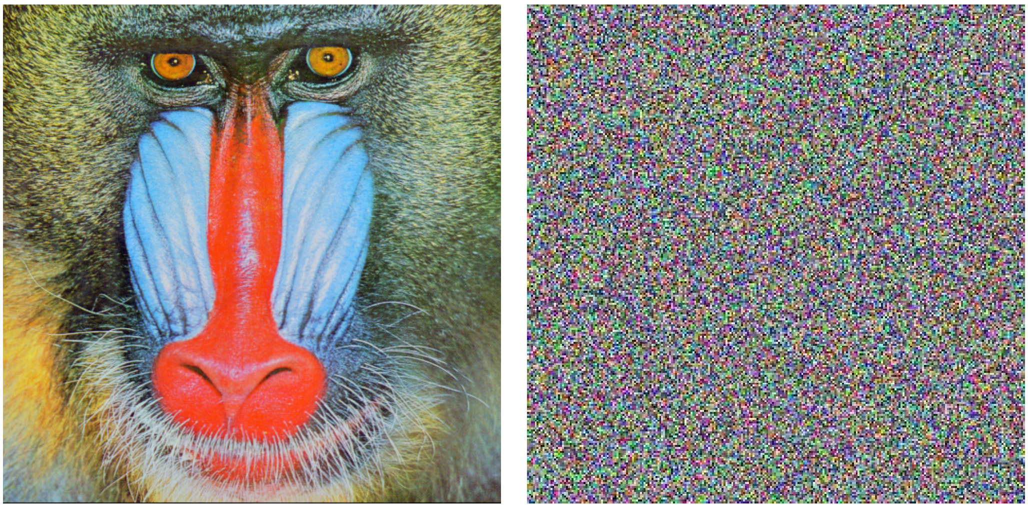
A histogram of an image shows the frequency distribution of its pixels. In order to have a strong encryption scheme, the histogram of an encrypted image must be uniform. This is because a uniform histogram distribution shows that the probability of each of the gray levels of the image is almost the same, thus rendering the image more resistant against statistical attacks. The histograms shown in Figures 11–13 depict histograms of each of the color channels of the encrypted Lena image. As can be seen, histograms of the encrypted images are uniform, unlike histograms of plain images, which have many sharp peaks. Hence, encrypted image pixels are distributed uniformly, resulting in images that do not reveal any statistical characteristics. This makes it extremely difficult for attackers to recover the plain image from its encrypted version.



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

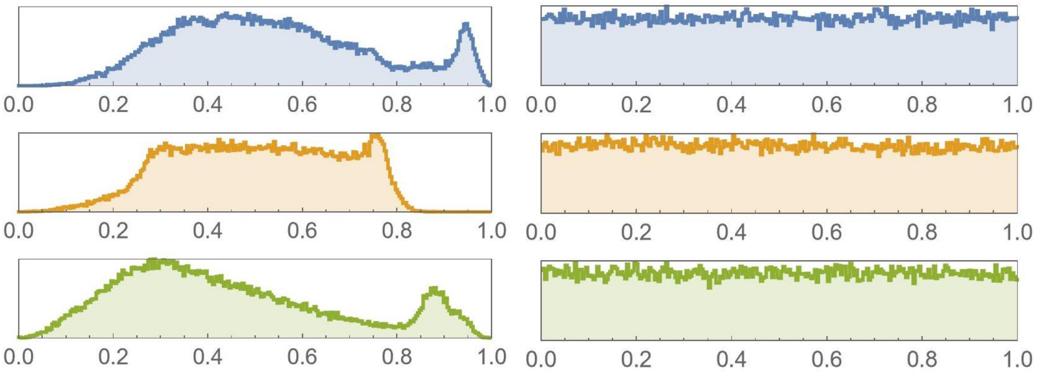
(**c**) (**d**)

Figure 12. Peppers image and histogram comparison before and after encryption. (**a**) Plain image. (**b**) Encrypted image. (**c**) Histogram of the plain image. (**d**) Histogram of the encrypted image.



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

Figure 13. *Cont.*



(**c**) (**d**)

Figure 13. Baboon image and histogram comparison before and after encryption. (**a**) Plain image. (**b**) Encrypted image. (**c**) Histogram of the plain image. (**d**) Histogram of the encrypted image.

4.2. Chi-Square Test

The histogram is approximated by a uniform distribution. The uniformity is verified by χ^2 test as expressed in (15),

$$\chi^2 = \sum_{k=1}^{256} \frac{(v_k - e_k)^2}{e_k} \tag{15}$$

where k is the number of gray levels, which is 256, and v_k is the observed occurrence frequencies of each gray level, from 0 to 255. Note that the expected occurrence frequency of each gray level is 256 [54]. For a significance level of 0.05, the computed χ^2 value of the encrypted Lena image of our proposed scheme is 289. Because $\chi^2_{test} < \chi^2_{255,0.05}$, this implies that the null hypothesis is not rejected and the distribution of the encrypted histogram is uniform [55]. Furthermore, our computed χ^2 value is superior to that of other image encryption schemes in the literature [56,57].

4.3. Information Entropy

Information entropy is employed to measure the randomness of the distribution of gray pixel values of an image. It is represented as the following expression according to Shannon's theory:

$$H(m) = \sum_{i=1}^{M} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{16}$$

where $p(m_i)$ refers to the probability of occurrence of symbol m, and M represents the total number of bits for each symbol. Theoretically, the entropy value of a randomly encrypted image is 8 because a gray scale image has 256 symbols and the data of the pixel have 2^8 possible combinations. The entropy values of the encrypted Lena, Peppers, and Baboon images are shown in Table 2. As can be seen, each of the values is a little over 7.99, which reveals that the proposed encryption scheme randomizes the distribution of the pixels of the plain image, making it impossible for an attacker to gain any information about the plain image from its encrypted version. Moreover, Tables 3 and 4 show entropy values of the RGB color channels of various images and how they compare with achieved values in the literature, respectively. It can be seen that the achieved entropy values are all a little over 7.99, very close to the ideal entropy value of 8 and comparable to the literature.

Table 2. Information entropy values of various images.

Image	Information Entropy
Lena	7.99910
Peppers	7.99877
Baboon	7.99907

Table 3. Information entropy values of the RGB color channels of various images.

Image	Channels	Information Entropy
Lena	Red Green Blue	7.9972 7.9973 7.9966
Peppers	Red Green Blue	7.9964 7.9969 7.9969
Baboon	Red Green Blue	7.9973 7.9967 7.9967

Table 4. Comparison of information entropy values of the RGB color channels of the Lena image.

Scheme	Information Entropy Values		
	Red	Green	Blue
Proposed scheme	7.9972	7.9973	7.9966
[46]	7.9991	7.9954	7.9963
[35]	7.9973	7.9972	7.9975
[58]	7.9994	7.9994	7.9993
[59]	7.9791	7.9802	7.9827
[60]	7.9948	7.9958	7.9950
[61]	7.9993	7.9993	7.9993

4.4. Mean Squared Error

The mean squared error (MSE) is utilized to measure the reliability of the proposed scheme. It is evaluated through comparing the plain and encrypted images' pixels, in order to detect any similarities or differences between them. Mathematically, it is expressed as:

$$\text{MSE} = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(P_{(i,j)} - E_{(i,j)})^2}{M \times N}, \tag{17}$$

where $P_{(i,j)}$ represents a pixel of the plain image and $E_{(i,j)}$ represents a pixel of the encrypted image. The product $M \times N$ gives the total number of pixels in any of the images. Theoretically, the value of the MSE must be a large number in order to have a scheme that is robust against any statistical attacks. Tables 5 and 6 show the computed MSE values for various encrypted images, as well as compares those of other schemes from the literature, respectively. It can be seen that the MSE values computed for encrypted images employing the proposed scheme are comparable or superior to those obtained from other schemes in the literature.

4.5. Peak Signal to Noise Ratio

The quality of the encryption scheme can be evaluated using the peak signal to noise ratio (PSNR), which is a ratio of the highest pixel value of the image over the MSE. Mathematically, it is expressed by:

$$PSNR = 10\log\left(\frac{I_{max}^2}{MSE}\right), \tag{18}$$

where I_{max} is the maximum pixel value, which is 255. The theoretical value of the PSNR should be as low as possible, as it is inversely proportional to the MSE. The lower the PSNR values, the better indication of the quality of the encryption scheme. Tables 5 and 6 show the computed PSNR values for various encrypted images and compares those of other schemes from the literature, respectively. It can be seen that the PSNR values computed for encrypted images employing the proposed scheme are comparable or superior to those obtained from other schemes in the literature.

Table 5. MSE and PSNR values of different image channels.

Image	Channels	MSE	PSNR [dB]
Lena	Red	10,663.2963	7.8518
	Green	8982.0206	8.5970
	Blue	7021.3295	9.6666
Peppers	Red	8032.5074	9.0822
	Green	11,143.3106	7.66066
	Blue	11,101.1624	7.67712
Baboon	Red	8337.2601	8.92057
	Green	7434.5269	9.41827
	Blue	9113.8334	8.53379

Table 6. Average MSE and PSNR values of different images.

Image	Proposed Scheme		[35]		[36]	
	Avg. MSE	Avg. PSNR [dB]	MSE	PSNR [dB]	MSE	PSNR [dB]
Lena	8888.88	8.64233	10,869.73	7.7677	4859.03	11.3
Peppers	10,092.3	8.09089	-	-	6399.05	10.10
Baboon	8295.21	8.94253	10,930.33	7.7447	7274.44	9.55

4.6. Mean Absolute Error

The mean absolute error (MAE) is a metric employed to measure the performance of the encryption scheme against differential attacks. The value of the MAE between an encrypted and a plain image must be large to guarantee that an encryption scheme is robust. It is mathematically expressed as:

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} P_{(i,j)} - E_{(i,j)}, \tag{19}$$

where $P_{(i,j)}$ refers to a pixel in the plain image and $E_{(i,j)}$ refers to a pixel in the encrypted image, in row i and column j; M and N are the dimensions of the image. Table 7 shows that the computed MAE values of the proposed scheme are comparable or superior to its counterparts from the literature.

Table 7. MAE analysis of the Lena, Peppers, and Baboon images.

Image	Proposed Scheme	[35]	[62]
Lena	77.3752	87	77.35
Peppers	81.7740	-	74.71
Baboon	75.1659	92	73.91

4.7. Correlation Coefficient Analysis

A correlation coefficient measures the similarity or difference between adjacent image pixels in three directions: vertically, horizontally, and diagonally. In order to have an image encryption scheme that is cryptographically secure, a strong correlation between the adjacent pixels in all directions should be eliminated. The value of the correlation coefficient ranges from −1 to 1, such that −1 means that it has a negative correlation, +1 means that it has a positive correlation, whereas 0 corresponds to no correlation. Therefore, the encrypted image must have a correlation coefficient close to 0 between the adjacent pixels in all the directions so it would resist statistical attacks. It is mathematically expressed as:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{20}$$

where

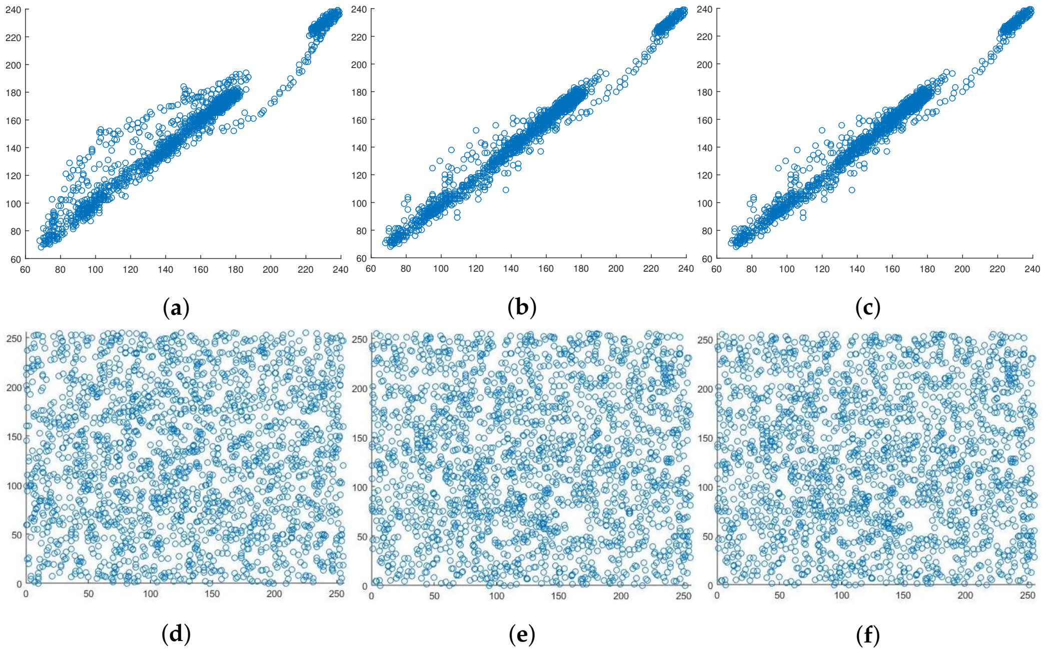
$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{21}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{22}$$

and

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i). \tag{23}$$

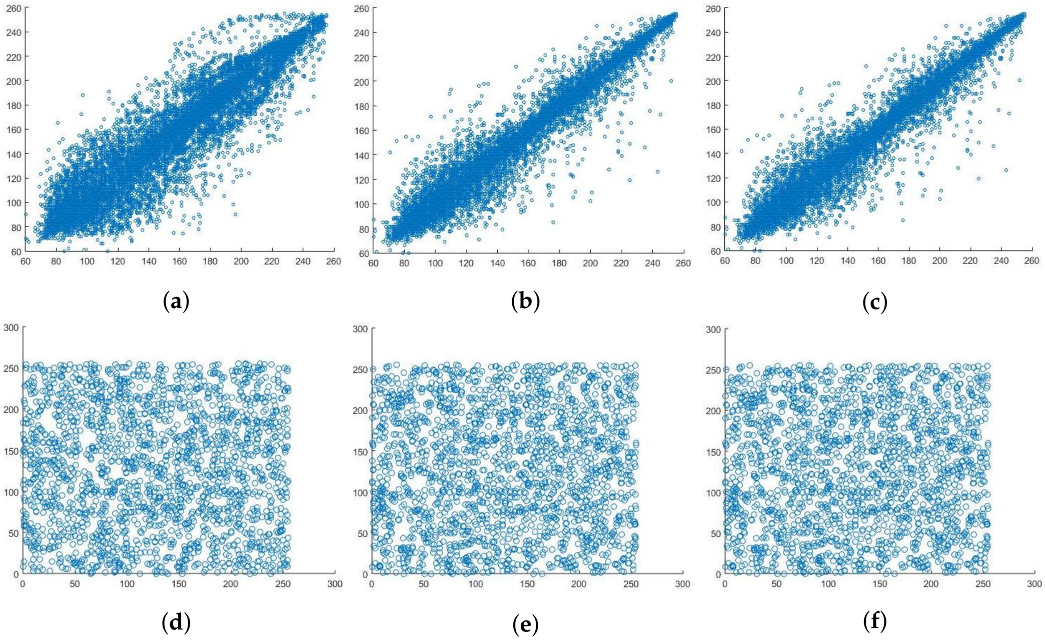
Figure 14 shows correlation coefficient plots of the plain and encrypted Lena image. As can be seen, the horizontal, vertical, and diagonal correlation coefficients of the adjacent pixels are linear. Moreover, the horizontal, vertical, and diagonal correlation coefficients plots of the encrypted image are uniform and have a scatter-like distribution. This same pixel correlation coefficient behavior can be seen in Figures 15–17, for the red, green, and blue channels of the Lena image, respectively. A set of 20,000 adjacent pixels were chosen along the horizontal, vertical, and diagonal directions for this computation. The distribution of the pixels in the plain image is linear and lies on the main diagonal. This indicates that the pixels are linearly correlated. In contrast, the pixel distribution of the encrypted image is more scattered, indicating the absence of correlation between the adjacent pixels.



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

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

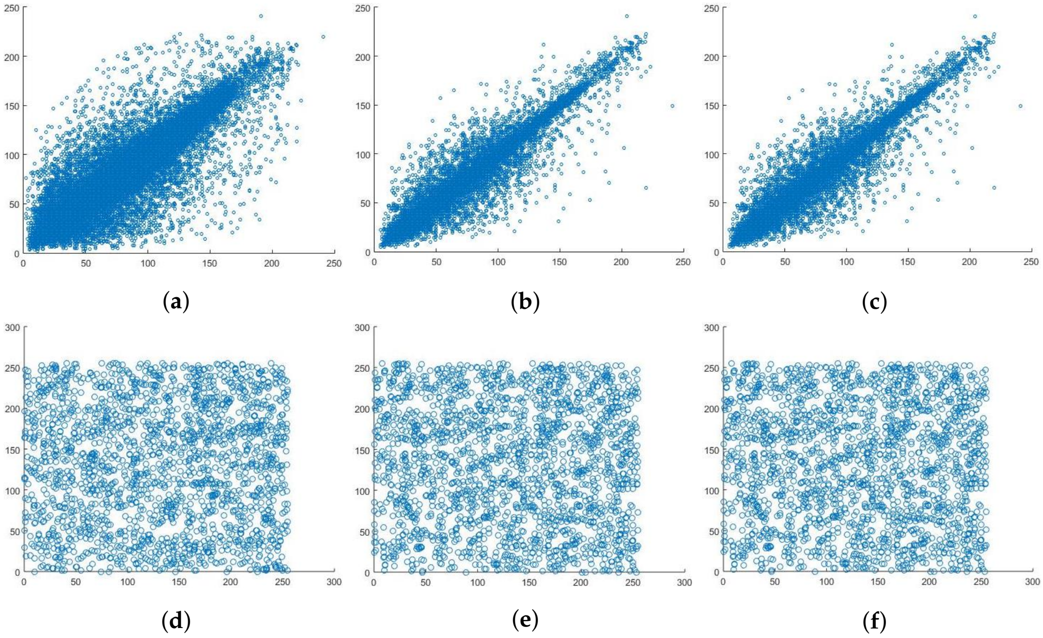
Figure 14. Correlation coefficient diagrams of the plain and encrypted Lena image. (**a**) Horizontal. (**b**) Vertical. (**c**) Diagonal. (**d**) Horizontal. (**e**) Vertical. (**f**) Diagonal.



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

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

Figure 15. Correlation coefficient diagram of the plain and encrypted red channel of Lena image. (**a**) Horizontal. (**b**) Vertical. (**c**) Diagonal. (**d**) Horizontal. (**e**) Vertical. (**f**) Diagonal.

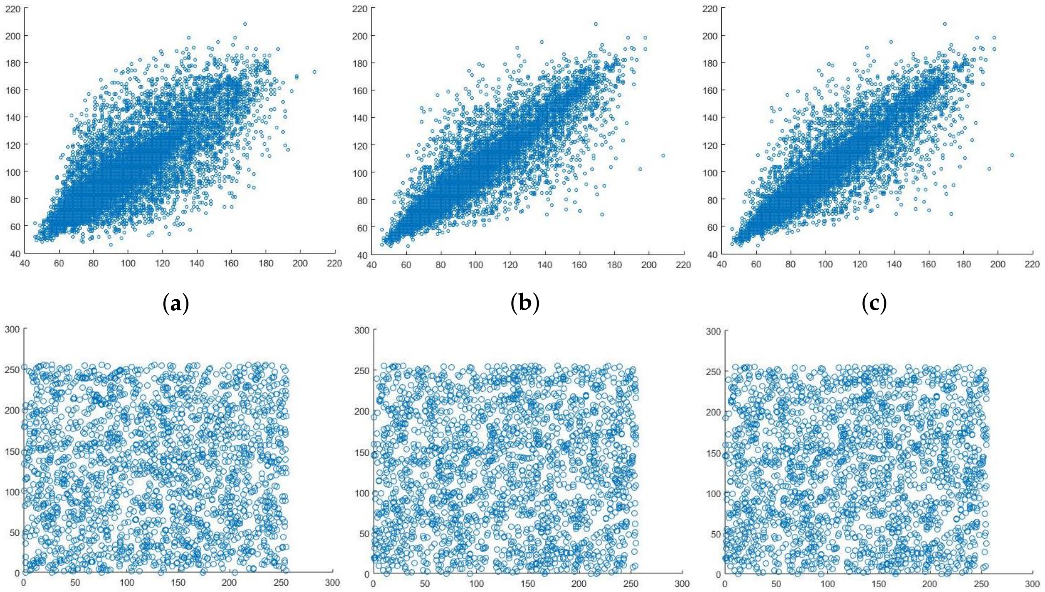


(**a**) (**b**) (**c**)

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

Figure 16. Correlation coefficient diagram of the plain and encrypted green channel of Lena image. (**a**) Horizontal. (**b**) Vertical. (**c**) Diagonal. (**d**) Horizontal. (**e**) Vertical. (**f**) Diagonal.

This linear relationship is also shown in Table 8, where the plain image has a correlation coefficient of $\sim$1 and the correlation coefficient of the encrypted image is $\sim$0, which means that the pixels are not correlated to one another, making the encrypted image meaningless to any attacker. Table 9 showcases a correlation coefficient comparison among the proposed scheme and some of its counterparts from the literature. It is clear that the results are comparable. A detailed correlation coefficient comparison in terms of each of the color channels is provided in Tables 10 and 11, for the Lena and Baboon images, respectively, as well as comparison with values from counterpart schemes from the literature.



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

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

Figure 17. Correlation coefficient diagram of the plain and encrypted blue channel of Lena image. (**a**) Horizontal. (**b**) Vertical. (**c**) Diagonal (**d**) Horizontal. (**e**) Vertical. (**f**) Diagonal.

Table 8. Correlation coefficients of plain and encrypted images.

	Plain Image			Encrypted Image		
	Correlation Coefficient			Correlation Coefficient		
Image	**Horizontal**	**Diagonal**	**Vertical**	**Horizontal**	**Diagonal**	**Vertical**
Lena	0.96734	0.94821	0.98276	0.002287	−0.00132	−0.00160
Peppers	0.95595	0.95371	0.97939	−0.00063	−0.00003	−0.00102
Baboon	0.92203	0.87049	0.90303	0.001362	−0.00332	−0.00138

Table 9. Correlation coefficients comparison between plain and encrypted Lena images.

Scheme	Horizontal	Diagonal	Vertical
Proposed scheme	0.002287	−0.00132	−0.00160
[24]	0.0022	−0.0017	0.0001
[35]	0.0054	0.0054	0.0016
[63]	0.000199	0.003705	−0.000924
[64]	0.0681	0.0128	0.0049
[65]	0.001862	0.003768	0.000710
[66]	−0.0082	−0.0012	−0.0128
[67]	0.000546	0.000192	0.000514
[68]	−0.0029	−0.0045	−0.0001
[69]	0.0023	−0.0059	0.0029

Table 10. Correlation coefficient comparison of plain and encrypted Lena image color channels.

		Lena				
Channel	**CC**	**Plain Image**	**Encrypted Image**	**[70]**	**[71]**	**[72]**
Red	HC	0.95722	−0.00364	0.001365	0.0021	0.9568
	DC	0.93389	0.00016	0.000232	−0.0026	0.0075
	VC	0.97889	0.000697	0.004776	0.0018	−0.0376
Green	HC	0.94321	0.000118	0.003294	−0.0006	0.0020
	DC	0.91931	0.00177	0.004807	0	−0.0046
	VC	0.97137	−0.0011	−0.000579	0.0004	−0.0013
Blue	HC	0.92845	−0.00164	0.002060	−0.005	0.0071
	DC	0.90068	−0.00523	−0.004043	−0.0104	−0.0009
	VC	0.95593	0.006041	0.000194	0.001	−0.0423

Table 11. Correlation coefficient comparison of plain and encrypted Baboon image color channels.

		Baboon			
Channel	**CC**	**Plain Image**	**Encrypted Image**	**[70]**	**[71]**
Red	HC	0.94741	−0.00428	0.001391	0.0005
	DC	0.90413	−0.00009	0.000334	0.0014
	VC	0.92152	0.000706	0.004650	0.0059
Green	HC	0.87266	0.00340	−0.008134	0.0078
	DC	0.79341	0.00282	0.005334	−0.001
	VC	0.83905	−0.0016	0.000829	0.0042
Blue	HC	0.92153	−0.00253	−0.00889	0.0021
	DC	0.87668	−0.00635	0.001710	−0.0114
	VC	0.91432	−0.00003	0.000056	−0.0039

4.8. Key Space Analysis

A key space analysis is carried out to compute the number of unique keys that can be utilized in the encryption process. In the proposed image encryption scheme, the secret keys and variables are assumed to be shared between the transmitter and receiver via a secure channel. In addition, the literature includes excellent key-establishment protocols, for example, [73]. In the proposed image encryption scheme, there is a total of eight variables. These are: P_μ and seven variables that are used to generate the keys, K_L and K_{CA}. The largest machine precision is 10^{-16}. Thus, the key space is approximately $10^{8\times16} = 10^{128} \approx 2^{425}$. This value exceeds the threshold earlier proposed in [74] as 2^{100}. This means that our proposed scheme can resist brute-force attacks. Furthermore, an examination of key space values of related image encryption schemes from the literature, as in Table 12, clearly indicates that the proposed scheme is larger than them.

Table 12. Key space values comparison.

Scheme	Key Space
Proposed scheme	$10^{128} \approx 2^{425}$
[31]	2^{256}
[38]	2^{345}
[39]	2^{256}
[32]	2^{128}
[63]	2^{187}
[75]	10^{94}
[76]	2^{128}
[77]	2^{219}

4.9. Differential Attack Analysis

A differential attack analysis is employed to measure the strength of the proposed encryption scheme against differential attacks. The number of pixels changing rate (NPCR) and the unified average change intensity (UACI) are two methods that are employed to carry out a differential attack analysis.

4.9.1. The Number of Pixel Changing Rate

The NPCR measures the number of pixels which are different between two images. It is mathematically expressed as:

$$NPCR = \frac{\sum_{i,j} D_{i,j}}{M \times N} \times 100, \tag{24}$$

where $D_{i,j}$ is given by:

$$D_{i,j} = \begin{cases} 0 & C_{1(i,j)} = C_{2(i,j)} \\ 1 & C_{1(i,j)} \neq C_{2(i,j)}. \end{cases} \tag{25}$$

4.9.2. The Unified Average Change Intensity

The UACI is a measure of the difference in the average intensity between the encrypted and plain images. It is mathematically expressed as:

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{C_{1(i,j)} - C_{2(i,j)}}{255}, \tag{26}$$

where $C_{1(i,j)}$ and $C_{2(i,j)}$ are two images of dimensions $M \times N$.

Table 13 depicts the NPCR and UACI results of the proposed encryption scheme on various images. As shown, the NPCR is greater than 99% and the UACI should also be greater than 33.35%. It is not in all the cases; however, it is close to it. As a result, any slight difference in the plain text image would result in a significant difference in the encrypted image. Moreover, the proposed scheme is also compared with its counterparts from the literature, in terms of the differential attacks. NPCR and UACI values are also shown in Tables 14 and 15. As can be seen, the computed NPCR value of the proposed scheme is >99% and is better than [35,78,79]. The UACI value should be ⩾33%, which is not the case for the proposed scheme, in which [78] is better.

Table 13. NPCR and UACI of different images.

Test Type	Image	Result
NPCR	Lena	99.62870
	Pepper	99.59360
	Baboon	99.58190
UACI	Lena	30.34321
	Pepper	32.17523
	Baboon	29.39764

4.10. Execution Time Analysis

The execution time is used to measure the complexity of this scheme and whether it can be used for real time applications. Table 16 shows the total execution time, in terms of encryption and decryption times, of the Lena image, provided for various dimensions. The total execution time ranges from 2.89 s to 16.217 s, depending on the image dimensions. Furthermore, Table 17 provides a comparison of the encryption time among the proposed image encryption scheme and its counterparts from the literature. Note that the differences in execution time depends on multiple factors, including the algorithm itself, the machine specifications on which the algorithm is run (i.e., processing power and available memory), as well as the software running the algorithm. Note that in [77,80–82], the software of choice is Mathworks Matlab®, whereas the proposed scheme is programmed on Wolfram Mathematica®. The average encryption time of the proposed image encryption scheme is 0.61 Mbps.

Table 14. NPCR and UACI of different image channels comparison.

Test Type	Image	Channel Type	Result	[83]
NPCR	Lena	Red	99.6109	99.6355
		Green	99.6109	99.6256
		Blue	99.6375	99.6159
	Pepper	Red	99.6032	99.6307
		Green	99.6032	99.6250
		Blue	99.3750	99.6213
	Baboon	Red	99.5880	99.6102
		Green	99.5880	99.6134
		Blue	99.5880	99.6057
UACI	Lena	Red	33.4158	33.4657
		Green	30.3902	33.4552
		Blue	33.2420	33.4550
	Pepper	Red	33.3459	33.4832
		Green	33.4702	33.4904
		Blue	33.4357	33.4619
	Baboon	Red	33.4273	33.5002
		Green	33.4635	33.4711
		Blue	33.7951	33.4951

Table 15. Average NPCR and UACI of the Lena image comparison.

Scheme	NPCR	UACI
Proposed scheme	99.62870	30.34321
[35]	99.52	26.7933
[78]	99.6075	33.4342
[79]	99.52	26.7933

Table 16. Encryption time of the proposed scheme for the Lena image at various dimensions.

Image Dimensions	t_{Enc} [s]	t_{Dec} [s]	t_{Tot} [s]
128 × 128	2.123165	0.76698	2.890163
256 × 256	2.582389	3.149124	5.731513
512 × 512	4.379808	11.83809	16.217898

Table 17. Execution time comparison for various schemes of the Lena image having dimensions 256 × 256.

Scheme	Encryption Time [s]	Machine Specifications (CPU and RAM)
Proposed scheme	2.582389	2.9 GHz Intel® Core™ i9, 32 GB
[77]	3.45	N/A
[80]	1.1168	3.4 GHz Intel® Core™ i7, 8 GB
[81]	1.112	3.4 GHz Intel® Core™ i3, 4 GB
[82]	4.98	2.5 GHz AMD®, 4 GB

4.11. The National Institute of Standards and Technology Analysis

A good PRNG should satisfy its randomness criteria by a number of tests that comprise the NIST analysis suite. Specifically, the probability, or p-value, of each of the tests should be greater than 0.01 for any bitstream to be regarded as random. The proposed encryption scheme is subjected to the NIST suite of tests, over a large number of lengthy bit sequences, and successfully passes each of them. As an illustration, Table 18 shows the results of the NIST analysis of each of the color channels of the encrypted Lena image. It is clear that the values for all the tests are indeed larger than 0.01, indicating the success of the proposed image encryption scheme at passing the NIST analysis.

Table 18. NIST analysis on the RGB color channels of the encrypted Lena image.

Test Name	Red	Green	Blue	Remarks
Frequency	0.612882	0.273620	0.426467	Success
Block Frequency	0.431942	0.338326	0.545500	Success
Run (m = 75,221)	0.239030	0.252482	0.103463	Success
Long runs of ones	0.907470	0.993509	0.650024	Success
Rank	0.839897	0.669290	0.934658	Success
Spectral FFT	0.504492	0.722283	0.962204	Success
Non overlapping	0.611940	0.669954	0.552968	Success
Overlapping	0.491780	0.502543	0.554045	Success
Universal	0.431557	0.016275	0.375857	Success
Serial	0.750796	0.094145	0.836764	Success
Serial	0.786736	0.214226	0.637876	Success
Approx. Entropy	0.701255	0.182486	0.781052	Success
Cumulative sum forward	0.941731	0.455203	0.368786	Success
Cumulative sum reverse	0.534965	0.347123	0.551838	Success

5. Conclusions

This paper proposed an RGB image encryption scheme that makes use of Shannon’s ideas of confusion and diffusion. The proposed scheme is implemented in three stages. In the first stage, Rule 30 cellular automaton is utilized to generate the first key. In the second stage, a well-designed S-box is utilized to create the needed non-linearity and complexity. Finally, in the third stage, a solution of the Lorenz system is used to generate the second key. The performance of the scheme was evaluated utilizing different metrics, statistically and differentially. Those included a histogram analysis and its associated χ^2 computations, a correlation coefficient analysis, MSE, PSNR, MAE, information entropy, an execution time analysis, a differential attack analysis (in terms of NPCR and UACI), a key space analysis, and a NIST analysis. The computed results suggest that the proposed scheme is resistant against any statistical, differential, or brute-force attacks. Moreover, on carrying out comparisons with counterpart image encryption schemes from the literature, the proposed color image encryption scheme exhibited either a comparable or a superior security performance. Nevertheless, the proposed scheme does not come without limitations. The Lorenz system utilized in the third stage is dissipative and has a comparatively poor ergodic property in comparison with conservative chaotic dynamical systems. Such systems have improved distribution in phase space while also exhibiting high ergodicity, sometimes at the expense of being more computationally complex. Future work could tackle this issue, attempting to find a dynamical system with a trade-off among high ergodicity, improved distribution in phase space, and low computational complexity.

Author Contributions: Conceptualization, W.A.; formal analysis, W.A.; investigation, M.E.; methodology, W.A., M.E. and A.A.; project administration, W.A.; software, W.A. and M.E.; supervision, W.A. and A.A.; visualization, W.A.; writing—original draft, W.A. and M.E.; writing—review and editing, W.A. and A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Farrag, S.; Maher, E.; El-Mahdy, A.; Dressler, F. Performance Analysis of UAV Assisted Mobile Communications in THz Channel. *IEEE Access* **2021**, *9*, 160104–160115. [CrossRef]
2. Furqan, H.M.; Solaija, M.S.J.; Türkmen, H.; Arslan, H. Wireless Communication, Sensing, and REM: A Security Perspective. *IEEE Open J. Commun. Soc.* **2021**, *2*, 287–321. [CrossRef]
3. El Mahdy, A.; Alexan, W. A threshold-free LLR-based scheme to minimize the BER for decode-and-forward relaying. *Wirel. Pers. Commun.* **2018**, *100*, 787–801. [CrossRef]
4. Moussa, Y.; Alexan, W. Message Security Through AES and LSB Embedding in Edge Detected Pixels of 3D Images. In Proceedings of the 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES), Giza, Egypt, 24–26 October 2020; pp. 224–229. [CrossRef]
5. Alexan, W.; Mamdouh, E.; Elkhateeb, A.; Al-Seba'ey, F.; Amr, Z.; Khalil, H. Securing Sensitive Data Through Corner Filters, Chaotic Maps and LSB Embedding. In Proceedings of the 2021 3rd Novel Intelligent and Leading Emerging Sciences Conference (NILES), Giza, Egypt, 23–25 October 2021; pp. 359–364.
6. Elkandoz, M.T.; Alexan, W. Logistic Tan Map Based Audio Steganography. 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; pp. 1–5. [CrossRef]
7. Mihailescu, M.I.; Nita, S.L. Big Data Cryptography. In *Pro Cryptography and Cryptanalysis*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 379–400.
8. Alexan, W.; El Beheiry, M.; Gamal-Eldin, O. A comparative study among different mathematical sequences in 3d image steganography. *Int. J. Comput. Digit. Syst.* **2020**, *9*, 545–552. [CrossRef]
9. Farrag, S.; Alexan, W. Secure 3D data hiding technique based on a mesh traversal algorithm. *Multimed. Tools Appl.* **2020**, *79*, 29289–29303. [CrossRef]
10. El-Shafai, W.; Almomani, I.M.; Alkhayer, A. Optical Bit-Plane-Based 3D-JST Cryptography Algorithm With Cascaded 2D-FrFT Encryption for Efficient and Secure HEVC Communication. *IEEE Access* **2021**, *9*, 35004–35026. [CrossRef]
11. Verbauwhede, I. The cost of cryptography: Is low budget possible? In Proceedings of the 2011 IEEE 17th International On-Line Testing Symposium, Athens, Greece, 13–15 July 2011; p. 133. [CrossRef]
12. Rifa-Pous, H.; Herrera-Joancomartí, J. Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet* **2011**, *3*, 31–48. [CrossRef]
13. Lu, Q.; Zhu, C.; Deng, X. An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access* **2020**, *8*, 25664–25678. [CrossRef]
14. Hosny, K.M. *Multimedia Security Using Chaotic Maps: Principles and Methodologies*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 884.
15. Wolfram, S. *A New Kind of Science*; Wolfram Media: Champaign, IL, USA, 2002; Volume 5.
16. Wen, C.; Li, X.; Zanotti, T.; Puglisi, F.M.; Shi, Y.; Saiz, F.; Antidormi, A.; Roche, S.; Zheng, W.; Liang, X.; et al. Advanced Data Encryption using 2D Materials. *Adv. Mater.* **2021**, *33*, 2100185. [CrossRef]
17. Tulli, D.; Abellan, C.; Amaya, W. Engineering High-Speed Quantum Random Number Generators. In Proceedings of the 2019 21st International Conference on Transparent Optical Networks (ICTON), Angers, France, 9–13 July 2019. [CrossRef]
18. Zhang, Y.; Lo, H.P.; Mink, A.; Ikuta, T.; Honjo, T.; Takesue, H.; Munro, W.J. A simple low-latency real-time certifiable quantum random number generator. *Nat. Commun.* **2021**, *12*, 1056. [CrossRef]
19. Tomassini, M.; Perrenoud, M. Cryptography with cellular automata. *Appl. Soft Comput.* **2001**, *1*, 151–160. [CrossRef]
20. Wolfram, S. Cryptography with cellular automata. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 18–22 August 1985; pp. 429–432.
21. Nandi, S.; Kar, B.K.; Chaudhuri, P.P. Theory and applications of cellular automata in cryptography. *IEEE Trans. Comput.* **1994**, *43*, 1346–1357. [CrossRef]
22. Yampolskiy, R.V.; Rebolledo-Mendez, J.D.; Hindi, M.M. Password protected visual cryptography via cellular automaton rule 30. In *Transactions on Data Hiding and Multimedia Security IX*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 57–67.
23. Chai, X.; Gan, Z.; Yang, K.; Chen, Y.; Liu, X. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Process. Image Commun.* **2017**, *52*, 6–19. [CrossRef]
24. Niyat, A.Y.; Moattar, M.H.; Torshiz, M.N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.* **2017**, *90*, 225–237. [CrossRef]
25. Jiao, K.; Ye, G.; Mei, Q. Image Encryption Scheme Based on Quantum Logistic Map and Cellular Automata. In Proceedings of the 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 23–26 April 2021; pp. 375–379. [CrossRef]
26. Li, W.; Li, J.; Guo, L. An Efficient 2bits-Level for Image Encryption Based on Dna, Multi-Delayed Chebyshev Map and Cellular Automata. In Proceedings of the 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 14–16 December 2018; pp. 131–137. [CrossRef]
27. Ben Slimane, N.; Aouf, N.; Bouallegue, K.; Machhout, M. Hash Key-Based Image Cryptosystem Using Chaotic Maps and Cellular Automata. In Proceedings of the 2018 15th International Multi-Conference on Systems, Signals Devices (SSD), Yasmine Hammamet, Tunisia, 19–22 March 2018; pp. 190–194. [CrossRef]

28. Kumari, M.; Gupta, S. Performance comparison between Chaos and quantum-chaos based image encryption techniques. *Multimed. Tools Appl.* **2021**, *80*, 33213–33255. [CrossRef] [PubMed]
29. Arroyo, D.; Diaz, J.; Rodriguez, F. Cryptanalysis of a one round chaos-based substitution permutation network. *Signal Process.* **2013**, *93*, 1358–1364. [CrossRef]
30. Elkandoz, M.T.; Alexan, W.; Hussein, H.H. Logistic Sine Map Based Image Encryption. In Proceedings of the 2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, Poland, 18–20 September 2019; pp. 290–295. [CrossRef]
31. Yang, B.; Liao, X. A new color image encryption scheme based on logistic map over the finite field ZN. *Multimed. Tools Appl.* **2018**, *77*, 21803–21821. [CrossRef]
32. Liu, H.; Jin, C. A novel color image encryption algorithm based on quantum chaos sequence. *3D Res.* **2017**, *8*, 4. [CrossRef]
33. ElKamchouchi, D.H.; Mohamed, H.G.; Moussa, K.H. A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion. *Entropy* **2020**, *22*, 180. [CrossRef]
34. Kumar, V.; Girdhar, A. A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach. *Multimed. Tools Appl.* **2021**, *80*, 3749–3773. [CrossRef]
35. Khan, M.; Masood, F. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimed. Tools Appl.* **2019**, *78*, 26203–26222. [CrossRef]
36. 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]
37. Seyedzadeh, S.M.; Norouzi, B.; Mosavi, M.R.; Mirzakuchaki, S. A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. *Nonlinear Dyn.* **2015**, *81*, 511–529. [CrossRef]
38. Ge, B.; Chen, X.; Chen, G.; Shen, Z. Secure and Fast Image Encryption Algorithm Using Hyper-Chaos-Based Key Generator and Vector Operation. *IEEE Access* **2021**, *9*, 137635–137654. [CrossRef]
39. Gao, H.; Wang, X. Chaotic Image Encryption Algorithm Based on Zigzag Transform With Bidirectional Crossover From Random Position. *IEEE Access* **2021**, *9*, 105627–105640. [CrossRef]
40. Ahmad, M.; Chugh, H.; Goel, A.; Singla, P. A chaos based method for efficient cryptographic S-box design. In Proceedings of the International Symposium on Security in Computing and Communication, Mysore, India, 22–24 August 2013; pp. 130–137.
41. Tanyildizi, E.; Özkaynak, F. A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps. *IEEE Access* **2019**, *7*, 117829–117838. [CrossRef]
42. Ahmad, M.; Al-Solami, E.; Alghamdi, A.M.; Yousaf, M.A. Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures. *IEEE Access* **2020**, *8*, 110397–110411. [CrossRef]
43. Zahid, A.H.; Al-Solami, E.; Ahmad, M. A novel modular approach based substitution-box design for image encryption. *IEEE Access* **2020**, *8*, 150326–150340. [CrossRef]
44. Khalid, I.; Jamal, S.S.; Shah, T.; Shah, D.; Hazzazi, M.M. A Novel Scheme of Image Encryption Based on Elliptic Curves Isomorphism and Substitution Boxes. *IEEE Access* **2021**, *9*, 77798–777810. [CrossRef]
45. Ramzan, M.; Shah, T.; Hazzazi, M.M.; Aljaedi, A.; Alharbi, A.R. Construction of S-Boxes using Different Maps over Elliptic Curves for Image Encryption. *IEEE Access* **2021**, *9*, 157106–157123. [CrossRef]
46. Tanveer, M.; Shah, T.; Rehman, A.; Ali, A.; Siddiqui, G.F.; Saba, T.; Tariq, U. Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box. *IEEE Access* **2021**, *9*, 73924–73937. [CrossRef]
47. Nizam Chew, L.C.; Ismail, E.S. S-box construction based on linear fractional transformation and permutation function. *Symmetry* **2020**, *12*, 826. [CrossRef]
48. Jamal, S.S.; Shah, T.; AlKhaldi, A.H.; Tufail, M.N. Construction of new substitution boxes using linear fractional transformation and enhanced chaos. *Chin. J. Phys.* **2019**, *60*, 564–572. [CrossRef]
49. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
50. Zaitsev, D.A. A generalized neighborhood for cellular automata. *Theor. Comput. Sci.* **2017**, *666*, 21–35. [CrossRef]
51. Tomassini, M.; Sipper, M.; Perrenoud, M. On the generation of high-quality random numbers by two-dimensional cellular automata. *IEEE Trans. Comput.* **2000**, *49*, 1146–1151.
52. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
53. Sparrow, C. *The Lorenz Equations: Bifurcations, Chaos, and Strange Attractors*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012; Volume 41.
54. Khanzadi, H.; Eshghi, M.; Borujeni, S.E. Image encryption using random bit sequence based on chaotic maps. *Arab. J. Sci. Eng.* **2014**, *39*, 1039–1047. [CrossRef]
55. Kwok, H.; Tang, W.K. A fast image encryption system based on chaotic maps with finite precision representation. *Chaos Solitons Fractals* **2007**, *32*, 1518–1529. [CrossRef]
56. Etemadi Borujeni, S.; Eshghi, M. Chaotic image encryption design using tompkins-paige algorithm. *Math. Probl. Eng.* **2009**, *2009*, 762652. [CrossRef]
57. Revathy, K.; Thenmozhi, K.; Amirtharajan, R.; Praveenkumar, P. CR Assisted IE Guarded Authenticated Biomedical Image Transactions. *IEEE Photonics J.* **2018**, *10*, 1–13. [CrossRef]
58. Hasanzadeh, E.; Yaghoobi, M. A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys. *Multimed. Tools Appl.* **2019**, *79*, 7279–7297. [CrossRef]

59. Liu, H.; Wang, X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt. Commun.* **2011**, *284*, 3895–3903. [CrossRef]
60. Yang, F.; Mou, J.; Sun, K.; Cao, Y.; Jin, J. Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit. *IEEE Access* **2019**, *7*, 58751–58763. [CrossRef]
61. Huang, Y.; Huang, L.; Wang, Y.; Peng, Y.; Yu, F. Shape synchronization in driver-response of 4-D chaotic system and its application in image encryption. *IEEE Access* **2020**, *8*, 135308–135319. [CrossRef]
62. Khan, M.; Shah, T. An efficient chaotic image encryption scheme. *Neural Comput. Appl.* **2015**, *26*, 1137–1148. [CrossRef]
63. Wang, Y.; Wu, C.; Kang, S.; Wang, Q.; Mikulovich, V. Multi-channel chaotic encryption algorithm for color image based on DNA coding. *Multimed. Tools Appl.* **2020**, *79*, 18317–18342. [CrossRef]
64. Rhouma, R.; Meherzi, S.; Belghith, S. OCML-based colour image encryption. *Chaos Solitons Fractals* **2009**, *40*, 309–318. [CrossRef]
65. Liu, H.; Kadir, A. Asymmetric color image encryption scheme using 2D discrete-time map. *Signal Process.* **2015**, *113*, 104–112. [CrossRef]
66. Wu, X.; Wang, K.; Wang, X.; Kan, H.; Kurths, J. Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Process.* **2018**, *148*, 272–287. [CrossRef]
67. Norouzi, B.; Mirzakuchaki, S. A fast color image encryption algorithm based on hyper-chaotic systems. *Nonlinear Dyn.* **2014**, *78*, 995–1015. [CrossRef]
68. Wu, X.; Wang, K.; Wang, X.; Kan, H. Lossless chaotic color image cryptosystem based on DNA encryption and entropy. *Nonlinear Dyn.* **2017**, *90*, 855–875. [CrossRef]
69. Hua, Z.; Zhou, Y. Exponential chaotic model for generating robust chaos. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *51*, 3713–3724. [CrossRef]
70. Zhang, Y.Q.; He, Y.; Li, P.; Wang, X.Y. A new color image encryption scheme based on 2DNLCML system and genetic operations. *Opt. Lasers Eng.* **2020**, *128*, 106040. [CrossRef]
71. Jithin, K.; Sankar, S. Colour image encryption algorithm combining, Arnold map, DNA sequence operation, and a Mandelbrot set. *J. Inf. Secur. Appl.* **2020**, *50*, 102428. [CrossRef]
72. Rehman, A.U.; Firdous, A.; Iqbal, S.; Abbas, Z.; Shahid, M.M.A.; Wang, H.; Ullah, F. A Color Image Encryption Algorithm Based on One Time Key, Chaos Theory, and Concept of Rotor Machine. *IEEE Access* **2020**, *8*, 172275–172295. [CrossRef]
73. Boyd, C.; Mathuria, A.; Stebila, D. *Protocols for Authentication and Key Establishment*; Springer: Berlin/Heidelberg, Germany, 2003; Volume 1.
74. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]
75. Ur Rehman, A.; Liao, X.; Ashraf, R.; Ullah, S.; Wang, H. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik* **2018**, *159*, 348–367. [CrossRef]
76. Li, B.; Liao, X.; Jiang, Y. A novel image encryption scheme based on logistic map and dynatomic modular curve. *Multimed. Tools Appl.* **2018**, *77*, 8911–8938. [CrossRef]
77. Hu, X.; Wei, L.; Chen, W.; Chen, Q.; Guo, Y. Color image encryption algorithm based on dynamic chaos and matrix convolution. *IEEE Access* **2020**, *8*, 12452–12466. [CrossRef]
78. Wu, X.; Kurths, J.; Kan, H. A robust and lossless DNA encryption scheme for color images. *Multimed. Tools Appl.* **2018**, *77*, 12349–12376. [CrossRef]
79. Huang, C.K.; Nien, H.H. Multi chaotic systems based pixel shuffle for image encryption. *Opt. Commun.* **2009**, *282*, 2123–2127. [CrossRef]
80. Gong, L.; Qiu, K.; Deng, C.; Zhou, N. An image compression and encryption algorithm based on chaotic system and compressive sensing. *Opt. Laser Technol.* **2019**, *115*, 257–267. [CrossRef]
81. Zhang, X.; Wang, L.; Wang, Y.; Niu, Y.; Li, Y. An image encryption algorithm based on hyperchaotic system and variable-step Josephus problem. *Int. J. Opt.* **2020**, *2020*, 6102824. [CrossRef]
82. Xu, L.; Li, Z.; Li, J.; Hua, W. A novel bit-level image encryption algorithm based on chaotic maps. *Opt. Lasers Eng.* **2016**, *78*, 17–25. [CrossRef]
83. Slimane, N.B.; Aouf, N.; Bouallegue, K.; Machhout, M. A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model. *Multimed. Tools Appl.* **2018**, *77*, 30993–31019. [CrossRef]