sensors

MDPI

Article

A Novel Grayscale Image Encryption Scheme Based on the Block-Level Swapping of Pixels and the Chaotic System

Muhammad Hanif [1], Nadeem Iqbal [2], Fida Ur Rahman [3], Muhammad Adnan Khan [4,*], Taher M. Ghazal [5,6], Sagheer Abbas [7], Munir Ahmad [7], Hussam Al Hamadi [8] and Chan Yeob Yeun [9,*]

1 Riphah Institute of Informatics, Riphah International University, Malakand Campus, Islamabad 46000, Pakistan
2 Department of Computer Science and IT, University of Lahore, Lahore 54590, Pakistan
3 Department of Computer Science and IT, University of Malakand, Chakdara 18800, Pakistan
4 Department of Software, Gachon University, Seongnam 13120, Korea
5 College of Computer and Information Technology, American University in the Emirates, Dubai Academic City, Dubai 503000, United Arab Emirates
6 Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Malaysia
7 School of Computer Science, National College of Business Administration and Economics, Lahore 54000, Pakistan
8 College of Engineering and IT, University of Dubai, Dubai 14143, United Arab Emirates
9 Center for Cyber Physical Systems, Khalifa University, Abu Dhabi 127788, United Arab Emirates
* Correspondence: adnan@gachon.ac.kr (M.A.K.); chan.yeun@ku.ac.ae (C.Y.Y.)

Abstract: Hundreds of image encryption schemes have been conducted (as the literature review indicates). The majority of these schemes use pixels as building blocks for confusion and diffusion operations. Pixel-level operations are time-consuming and, thus, not suitable for many critical applications (e.g., telesurgery). Security is of the utmost importance while writing these schemes. This study aimed to provide a scheme based on block-level scrambling (with increased speed). Three streams of chaotic data were obtained through the intertwining logistic map (ILM). For a given image, the algorithm creates blocks of eight pixels. Two blocks (randomly selected from the long array of blocks) are swapped an arbitrary number of times. Two streams of random numbers facilitate this process. The scrambled image is further XORed with the key image generated through the third stream of random numbers to obtain the final cipher image. Plaintext sensitivity is incorporated through SHA-256 hash codes for the given image. The suggested cipher is subjected to a comprehensive set of security parameters, such as the key space, histogram, correlation coefficient, information entropy, differential attack, peak signal to noise ratio (PSNR), noise, and data loss attack, time complexity, and encryption throughput. In particular, the computational time of 0.1842 s and the throughput of 3.3488 Mbps of this scheme outperforms many published works, which bears immense promise for its real-world application.

Keywords: cryptography; encryption; image processing; cipher; information security

Citation: Hanif, M.; Iqbal, N.; Ur Rahman, F.; Khan, M.A.; Ghazal, T.M.; Abbas, S.; Ahmad, M.; Al Hamadi, H.; Yeun, C.Y. A Novel Grayscale Image Encryption Scheme Based on the Block-Level Swapping of Pixels and the Chaotic System. *Sensors* **2022**, *22*, 6243. https://doi.org/10.3390/s22166243

Academic Editors: Byung-Gyu Kim and Dongsan Jun

Received: 22 July 2022
Accepted: 17 August 2022
Published: 19 August 2022

1. Introduction

Different hardware and software products are changing the way we live. From telecommunications to natural language processing, from cloud server storage to artificial intelligence software, from robotics to varied computer vision applications—one can see the tremendous influences these products have on humanity. Moreover, digital cameras are all around us, which means pictures are being taken around the clock. Images are ubiquitous, e.g., in the form of selfies, family pictures, party pictures, pictures of different dignitaries, etc. Among these images, some are sensitive, e.g., images of spies in military and espionage settings or images of new products made by multinational companies. Storing these images on gadgets and transmitting them through public networks are risky since hackers seek

such activities. Hence, appropriate steps must be taken to safeguard these images. One traditional way is via encryption, in which plaintext is scrambled and diffused to convert it into some unrecognizable and cloudy format. For this purpose, some historical ciphers built by cryptographers are RSA, AES, and DES. Unfortunately, they work on text data only; digital images consist of pixels [1], which are tiny pieces of information that have intensity values in the range of 0 to 255. These pixels have strong correlations with each other and are highly redundant in character. Thus, new mechanisms are required for image encryptions that use these image characteristics.

In the literature, many image encryption schemes exist for grayscale [1–10] and color images [11–19]. Most of these encryption algorithms are based on chaotic maps. These systems/maps produce random data, which are utilized in encryption processes, including transposition (scrambling or confusion) and substitution (diffusion). These maps have the characteristics of randomness, unpredictability, ergodicity, aperiodicity, mixing, etc. They are fully dependent on their primary conditions and system parameters. Thus, they produce different streams of random numbers upon minute changes in their preconditions and parameters. This is why researchers have used them widely in designing their image encryption schemes [20–25]. In this study, the intertwining logistic chaotic map (ILM) is used to fulfill the requirements of chaoticity in the transposition and substitution processes. The ILM produces three chaotic streams and is much more unpredictable in nature [26].

As described earlier, the basic building blocks of encryption schemes are transposition and substitution. Upon surveying the image encryption literature—image encryption schemes were cracked because of the different vulnerabilities and weaknesses presented in their designs. The vulnerabilities were weak points that were ignored by cryptographers while designing their schemes. Few encryption schemes among them were based only on the transposition mechanism [27–29]. These mechanisms could not withstand the security attacks, such as known- and chosen plaintext attacks. In these encryption schemes, pixels are only shuffled in specific ways, which are usually quite predictable since each time the same procedure is adopted. Thus the attacker easily guesses the pattern and breaks the cipher [27]. To safeguard against these limitations, the new scheme for image encryption comprises both operations of transposition and substitution. After incorporating both of these operations, some image encryption schemes [30–32] were also broken through with different attacks [33–35], such as the differential attack, chosen cipher attack, and chosen plaintext attack, respectively. The main reason behind the breakages/weaknesses was that the chaotic data rendered through chaotic systems utilized in the schemes were not connected to the plain image. Thus, each time, the same data were generated, no matter which input image was used. The attacker figured out this pattern, which led to the breakage of the cipher. Plaintext sensitivity is a remedy to this attack [36–38].

Besides the concern of security, time efficiency was an important factor for researchers to deliver speedy products. In this regard, they resorted to different approaches, such as swapping mechanisms, circular shift operations, cellular automaton, block mechanisms, and so on. Many image encryption schemes were developed upon the notion of blocks also being produced [39–48]. In [39], the scheme for the encryption of images was presented based on the block-based transformation algorithm. The pixels were grouped into blocks. After that, scrambling operations were carried out by rotating them in the right direction using the XOR operation. Yet another image encryption using block cipher was introduced by [40]. The authors used chaotic sequences and adequate modes of operation, such as the counter mode and cipher block chaining. Their model was inspired by the Rijndael cipher. The security analysis showed that their algorithm was robust and had good security effects. The image encryption algorithm based on the theory of quantum was presented in [41]. In particular, their scheme was based on the quantum Arnold transformation (QAT) and the sine cation model (SCM). In this work, the image's gray pixel position information and the values of the image blocks were knitted into two qubit sequences. For the scrambling operation, the QAT was applied over the image blocks and the XOR operation was made over the scrambled image. Using the enhanced-logistic map (ELM) and modified zigzag

transformation, another block-based image encryption was proposed in [42]. The results demonstrated that their scheme could resist the various attacks of cryptanalysis.

Considering the literature review (as mentioned above), a new block image encryption scheme has been suggested, with the following highlights.

- The scheme is efficient regarding the computational time. Thus, it has good chances for its real-world application.
- This scheme has achieved better throughput. Moreover, the incorporation of plaintext sensitivity is a good way to avert the potential threats of cryptanalytic attacks.
- The majority of instructions of the suggested scheme are repetitive. Thus this scheme can be easily customized to run in some parallel settings.

The remainder of this paper is divided into five sections. In Section 2, the basic principles of block-level swapping and the chaotic system are discussed. The mechanisms for key stream generation and encryption/decryption procedures are discussed in Section 3. The simulation, security, and performance analyses using the varied validation metrics are presented in Sections 4 and 5. Finally, the concluding remarks are provided in Section 6.

2. Basic Principles

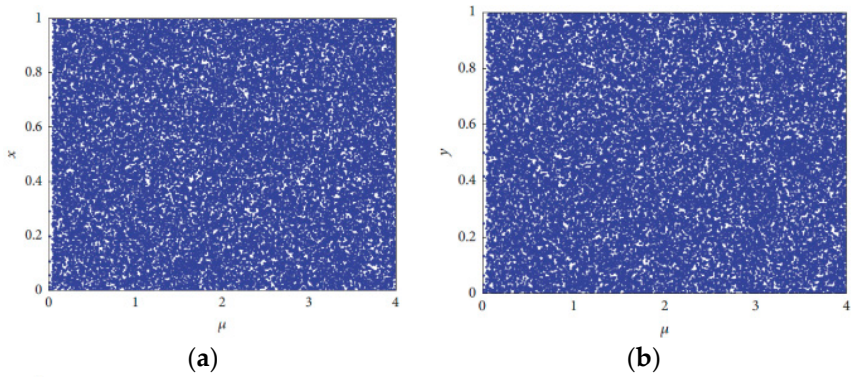
The basic working principles upon which the current work depends are discussed in this section.

2.1. Chaotic System

The chaos theory probes into the systems that are highly dynamical in their characters and orientations. Moreover, they are extremely sensitive to the two components. These are the system parameters and the initial values of the chaotic system/map. In this work, the intertwining logistic map (ILM) has been used [49].

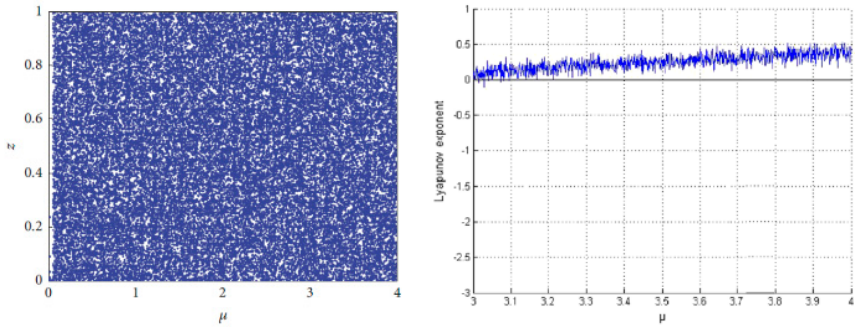
$$\begin{cases} l_{a+1} = [\mu \times k_1 \times m_n \times (1 - l_a) + n_a] mod\ 1 \\ m_{a+1} = \left[\mu \times k_2 \times m_a + n_a \times \frac{1}{(1+l_{a+1}^2)}\right] mod\ 1 \\ n_{a+1} = [\mu \times (l_{a+1} + m_{a+1} + k_3) \times sinn_a] mod\ 1 \end{cases} \quad (1)$$

In the above equation, $0 < \mu \leq 3.999$, $|k_1| > 33.500$, $|k_2| > 37.970$, and $|k_3| > 35.700$ are the initial values. The ILM produces three chaotic streams, (l, m, n) as can be seen in the above equation. This map is better than its antecedent logistic map since it has better chaoticity and contains no blank spaces [49]. This map has a desirable feature of chaoticity as this surpasses its predecessor maps. Additionally, there are no empty values and it has an even distribution as depicted in Figure 1a–c. Moreover, it has positive Lyapunov exponents, as shown in Figure 1d.



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

Figure 1. *Cont.*



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

Figure 1. Distribution of intertwining logistic map; (**a**) bifurcation diagram of sequences x; (**b**) bifurcation diagram of sequences y; (**c**) bifurcation diagram of sequences z; (**d**) Lyapunov exponents diagram.

2.2. Block Swapping

Blocks are fixed-size groups of pixels treated as one unit. They can help in improving the computational time of the cipher. In image encryption technology, a pixel is usually treated as a single unit, which is time-consuming. In contrast to that, the proposed scheme has treated 8 pixels as a single unit, dubbed a block. Figure 2 shows the block-wise swapping of the 8 pixels.

2	4	7	6	2	6	4	3	1	5	4	4
3	8	2	5	7	3	7	1	4	1	4	4
5	7	2	1	6	5	1	3	4	6	4	7
6	4	1	5	9	6	4	7	7	4	5	9
1	1	8	9	4	3	4	6	5	7	9	9
4	1	2	2	3	4	7	5	8	9	3	9
1	6	5	5	6	1	9	4	8	4	2	5
8	2	8	5	9	9	8	6	8	6	5	2
1	6	2	1	9	1	8	2	6	4	9	1
7	8	9	7	4	7	9	9	4	7	8	1
3	5	2	4	1	5	8	5	2	6	8	3
5	2	6	4	6	8	3	2	9	4	5	5

(**a**)

2	4	7	6	2	6	4	3	1	5	4	4
3	8	2	5	7	3	7	1	4	1	4	4
5	7	2	1	6	5	1	3	4	6	4	7
6	4	1	5	9	6	4	7	7	4	5	9
1	1	8	9	4	3	4	6	5	7	9	9
4	1	2	2	3	4	7	5	8	9	3	9
1	6	5	5	6	1	9	4	8	4	2	5
8	2	8	5	9	9	8	6	8	6	5	2
1	6	2	1	9	1	8	2	6	4	9	1
7	8	9	7	4	7	9	9	4	7	8	1
3	5	2	4	1	5	8	5	2	6	8	3
5	2	6	4	6	8	3	2	9	4	5	5

(**b**)

2	4	7	6	2	6	4	3	1	5	4	4
3	8	2	1	6	2	1	9	1	8	2	4
5	7	2	1	6	5	1	3	4	6	4	7
6	4	1	5	9	6	4	7	7	4	5	9
1	1	8	9	4	3	4	6	5	7	9	9
4	1	2	2	3	4	7	5	8	9	3	9
1	6	5	5	6	1	9	4	8	4	2	5
8	2	8	5	9	9	8	6	8	6	5	2
5	7	3	7	1	4	1	4	6	4	9	1
7	8	9	7	4	7	9	9	4	7	8	1
3	5	2	4	1	5	8	5	2	6	8	3
5	2	6	4	6	8	3	2	9	4	5	5

(**c**)

Figure 2. Block-swapping row-wise: (**a**) the initial state of the image; (**b**) the highlighted blocks; (**c**) the state of the image in (**a**) after block-swapping.

3. Proposed Block-Based Image Encryption Scheme

In this section, we discuss how the chaotic data were generated as well as the suggested scheme for the encryption of images.

3.1. Generation of the Initial Values and System Parameters

Two different types of keys are used in this scheme: a 256-bit hash code generated from the input image and a 256-bit user key given by the user. The hash key of the plain image helps in the realization of the plain text sensitivity. The hash key and the user key were mixed to generate the system parameters and the initial values of the chaotic map. Both the hash value and user key are split into four blocks of 64 bits each. The 256-bit hash value HV and User key UK are stated as follows:

$$HV = hv_1, hv_2, hv_3, hv_4. \tag{2}$$

$$UK = uk_1, uk_2, uk_3, uk_4. \tag{3}$$

subject to $hv_a = \{hv_{a,0}, hv_{a,1}, \ldots, hv_{a,63}\}$, where in $hv_{a,b}$, a denotes the character number and b denotes the bit number in $hv_{a,b}$. Analogously, in the User key UK: $uk_a = \{uk_{a,0}, uk_{a,1}, \ldots, uk_{a,63}\}$, where in $uk_{a,b}$, a denotes the character number and b denotes the bit number in $uk_{a,b}$. The following steps show the initial value and key stream generations for the ILM.

Step 1: Both the HV and UK are reshaped into 4×64 tables.

Step 2: The XOR operation is made between HV and UK, starting from the first row of the first table and the last row of the second table, as described by the following equations.

$$R_{1,b}{}' = HV_{1,b} \oplus UK_{4,b} \tag{4}$$

$$R_{2,b}{}' = HV_{2,b} \oplus UK_{3,b} \tag{5}$$

$$R_{3,b}{}' = HV_{3,b} \oplus UK_{2,b} \tag{6}$$

$$R_{4,b}{}' = HV_{4,b} \oplus UK_{1,b} \tag{7}$$

$$R' = R_{1,b}, R_{2,b}, R_{3,b}, R_{4,b} \tag{8}$$

where the symbol $\oplus$ represents the XOR operation. Moreover, $R_{1,b}{}'$ is the first row of the key table obtained after an XOR operation between $HV_{1,b}$ and $UK_{4,b}$. Similarly, other rows have been treated. Lastly, R' is the new 256-bit key value.

Step 3: After adding the values of columns for all four rows, we obtain the following:

$$\alpha = \sum_{b=1}^{8} R'(1,b) \tag{9}$$

$$\beta = \sum_{b=1}^{8} R'(2,b) \tag{10}$$

$$\gamma = \sum_{b=1}^{8} R'(3,b) \tag{11}$$

$$\delta = \sum_{b=1}^{8} R'(4,b) \tag{12}$$

Step 4: The equations below were used to calculate the ILM system parameters:

$$k_1 = \frac{\alpha \oplus \beta}{256} + 33.50 \tag{13}$$

$$k_2 = \frac{\gamma \oplus \delta}{256} + 37.90 \tag{14}$$

$$k_3 = \frac{(\alpha + \beta) \oplus (\gamma + \delta)}{256} + 35.70 \tag{15}$$

$$\mu = mod((\alpha + (\gamma/\delta) \times \beta),\ 4) \tag{16}$$

Step 5: The initial values of the ILM were calculated as

$$l_0 = mod((\mu \times (k_1 + k_2)/k_3),\ 0.5) \tag{17}$$

$$m_0 = mod((\mu \times (k_2 + k_3)/k_1),\ 0.5) \tag{18}$$

$$n_0 = mod((\mu \times (k_1 + k_3)/k_2), 2.5) \tag{19}$$

where $mod(y, z)$ calculates the remainder when z divides the y.

Step 6: The chaotic system (1) is repeated for $(MN + n_0)$ times to obtain three chaotic steams, i.e., l, m, n, where the $l = [l_1, l_2, \ldots, l_{MN+n0}]$, $m = [m_1, m_2, \ldots, m_{MN+n0}]$, $n = [n_1, n_2, \ldots, n_{MN+n0}]$. Here, MN are the resolutions of input images and $n_0 \geq 500$ are used for the removal of momentary effects from the chaotic map by ignoring the starting n_0 values.

Step 7: The three chaotic streams of ILM i.e., l, m, and n are further modified as follows.

$$block - selection1(i) = mod\left(floor\left(l(i) \times 10^{14}\right), NoB\right) \quad (20)$$

$$block - selection2(i) = mod\left(floor\left(m(i) \times 10^{14}\right), NoB\right) \quad (21)$$

$$key - image(i) = mod\left(floor\left(n(i) \times 10^{14}\right), 256\right) \quad (22)$$

where NoB denotes the number of blocks. Further, $block - selection1$, $block - selection2$, and $key - image$ are the new key streams according to the algorithmic logic we conceived. $i = 1, 2, \ldots, MN$.

3.2. Encryption Procedure

The proposed image encryption scheme is shown in Figure 3. The encryption procedure is explained in the steps below.

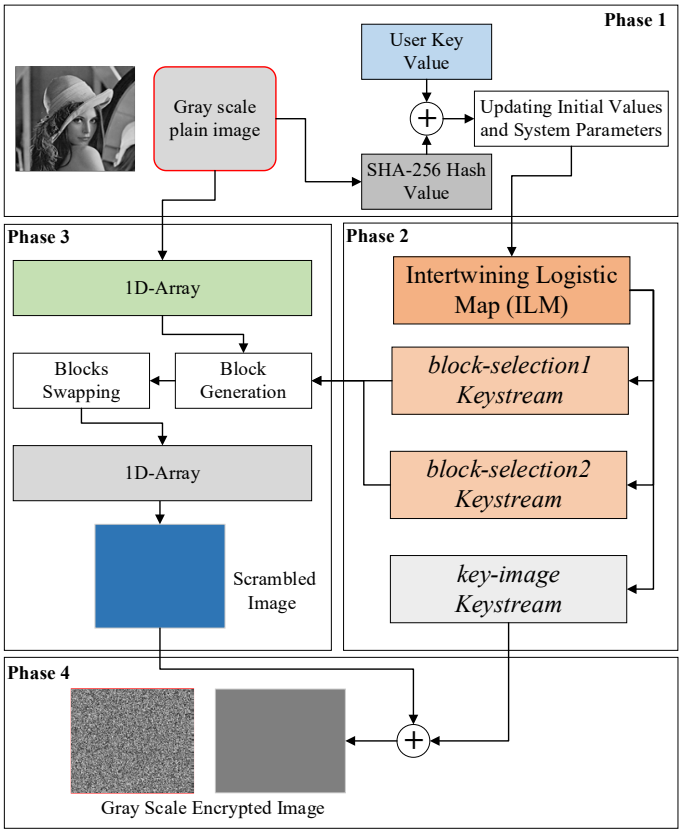


Figure 3. Block-based encryption scheme.

Step 1: This involves inputting the grayscale image and decomposing it into the 1D array. The grayscale plain image img of size $M \times N$ is input. The input image is then decomposed into the one-dimension (1D) array, i.e., $Array$. The size of this 1D array is $1 \times M \times N$.

Step 2: This involves decomposing the 1D array into blocks. Decompose the 1D array into blocks; each block size is 64 bits or 8 pixels. The total number of blocks is NoB, obtained as follows.

$$NoB = (1 \times M \times N)/8 \quad (23)$$

Step 3: Scrambling operation.

Step 3.1: Set the $index = 1$.

Step 3.2: Block selection. Select the first and second blocks and assign them to *bs1* and *bs2*, as follows.

$$bs1 = block - selection1(index) \times 8 + 1 \quad (24)$$

$$bs2 = block - selection2(index) \times 8 + 1 \quad (25)$$

Step 3.3: Swapping operation.

The following steps were carried out to perform the swapping operations over the selected blocks.

$$emp = Array(bs1 : bs1 + 8) \quad (26)$$

$$Array(bs1 : bs1 + 8) = Array(bs2 : bs2 + 8) \quad (27)$$

$$Array(bs2 : bs2 + 8) = temp \quad (28)$$

Here, the variable *Temp* was used to store the block of the pixels.

Step 3.4: $index = index + 1$.

Step 3.5: Repeat Steps 4.2, 4.3, and 4.4, while $index \leq MN$.

Step 3.6: Let $Array' = Array$.

$Array'$ is the scrambled image.

Step 4: Diffusion operation.

Diffusion effects were realized through the XOR operation between $Array'$ and the $key - image$.

$$Array''(a) = Array'(a) \oplus key - image(a) \quad (29)$$

where $a = 1, 2, \ldots, MN$. Reshape the image $Array''$ to $M \times N$ to obtain the final cipher image.

In the domain of cryptography, two approaches exist for the task of encryption, i.e., the private key and the public key. In this work, we adopted the former approach. Thus, the decryption procedure does not need to be explained in detail. This procedure would just be a reversal of the steps of the encryption procedure.

4. Simulation

A good cipher must be capable of handling a variety of attacks launched by potential antagonists. The differential attacks, chosen plaintext attack, brute force attack, entropy attack, cipher attack, statistical attack, and many others, are common in the realm of image encryption. To demonstrate it, eight grayscale images were chosen, each with a size of 256×256. The grayscale images were downloaded from the online repository of images using the link: http://sipi.usc.edu/database/ (accessed on 4 December 2021). The selected grayscale images were: Lena, baboon, bridge, cameraman, airplane, clock, moon, and ship. MATLAB version R2018a (64-bits), double-precision, was used (according to the IEEE [50] standard 754). The variable values used in the ILM were: $k_1 = 33.5$, $k_2 = 37.9$, $k_3 = 35.7$, $x_0 = 0$, $y_0 = 0$, $z_0 = 0$, $\mu = 0$. Figures 4–7 show the original plain (input) images, scrambled images, encrypted images, and decrypted images, respectively. These figures clearly show that the inputted plain images were converted into unrecognizable formats. The attacker would have no clue on how to retrieve the original input images from the scrambled and output encrypted images.

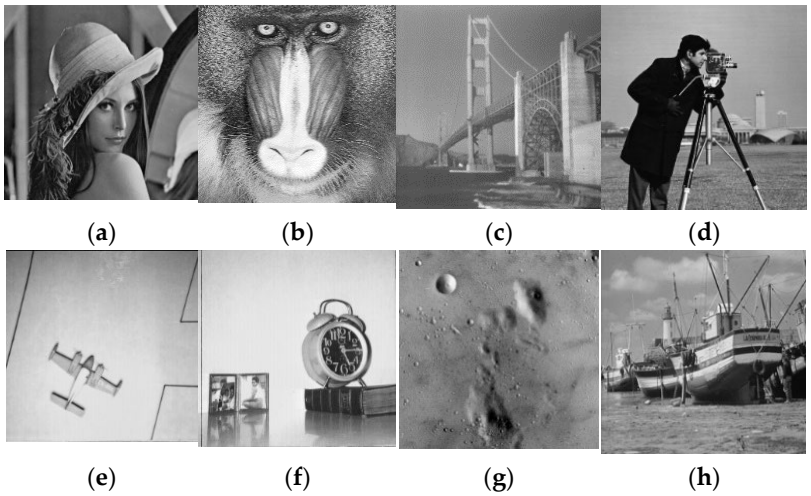


Figure 4. Original input images: (**a**) Lena; (**b**) baboon; (**c**) bridge; (**d**) cameraman; (**e**) airplane; (**f**) clock; (**g**) moon; (**h**) ship.

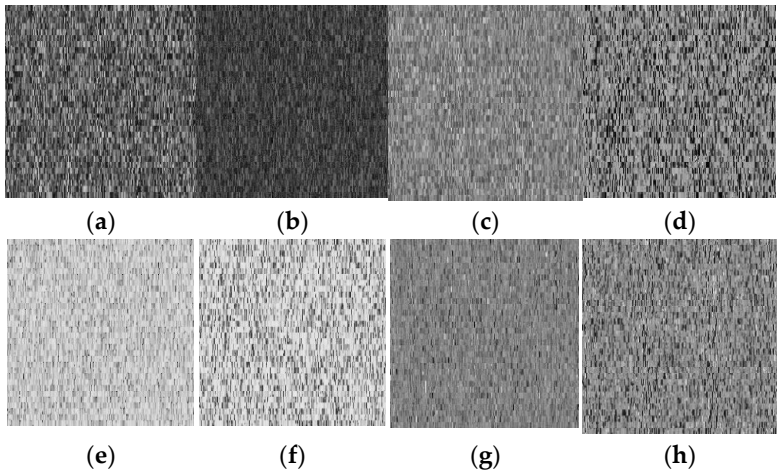


Figure 5. Scrambled images: (**a**) Lena; (**b**) baboon; (**c**) bridge; (**d**) cameraman; (**e**) airplane; (**f**) clock; (**g**) moon; (**h**) ship.

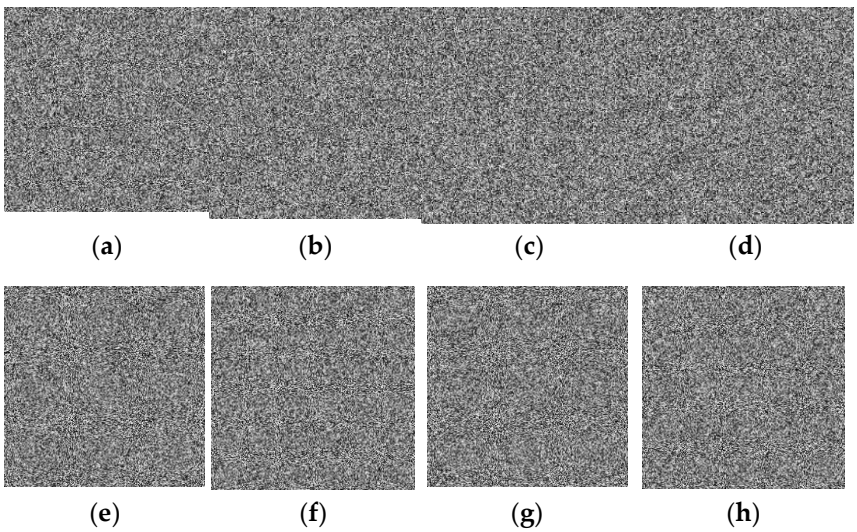


Figure 6. Encrypted images: (**a**) Lena; (**b**) baboon; (**c**) bridge; (**d**) cameraman; (**e**) airplane; (**f**) clock; (**g**) moon; (**h**) ship.

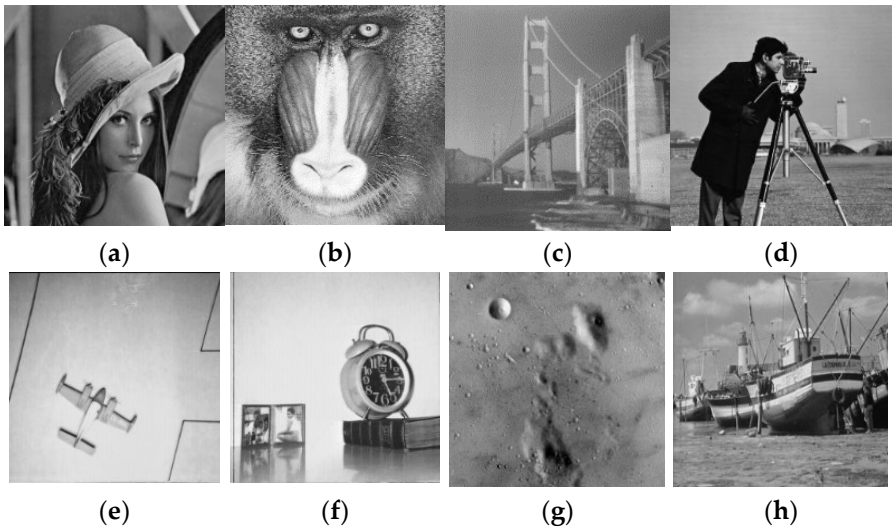


Figure 7. Decrypted images: (**a**) Lena; (**b**) baboon; (**c**) bridge; (**d**) cameraman; (**e**) airplane; (**f**) clock; (**g**) moon; (**h**) ship.

5. Security Analysis

In this section, the performance and security analyses based on different validation metrics are carried out.

5.1. Key Space Analysis

In any encryption scheme, one of the most important features is the key space. A large key space provides resistance against a brute force attack. There are four blocks. Each block consists of 64 bits, contributing $(2^{64})^4 = 2^{256}$ to the key space. Further, the ILM has four system parameters and three initial values making up seven variables. Moreover, 10^{-15} is taken as the computer precision. Thus, this contributes $(10^{15})^7 = 10^{105}$ to the key space. Therefore, the overall key space comes out as $2^{256} \times 10^{105} = 1.16 \times 10^{182}$. This value is sufficient to counter the brute force threat since it crosses the minimum threshold 2^{100} [17,22]. Table 1 highlights the key space of our proposed scheme and its comparison with other published works.

Table 1. Key space comparison between the proposed scheme and other schemes.

Algorithm	Key Space
Ours	1.16×10^{182}
[19]	10^{105}
[45]	$2^{197} \approx 2 \times 10^{59}$
[51]	10^{128}
[52]	10^{90}
[53]	$2^{197} \approx 2 \times 10^{59}$
[54]	$2^{199} \approx 8 \times 10^{59}$

5.2. Statistical Analysis

In image encryption technology, another significant metric is the statistical analysis. Two types of tests have been conducted by researchers, i.e., the histogram analysis and correlation coefficient analysis.

5.2.1. Histogram Analysis

In a given image, the pixel intensity value distribution is provided through the histogram. For a plain image, the histogram has slanting bars, which can be exploited by a hacker to obtain useful information about the image. To resist the statistical attack, a cipher must be capable of converting the slanting bars into a well-organized plain bar

with almost the same distribution. In this way, a hacker would not be able to obtain any useful information. The histograms of both plain and cipher images of Lena are shown in Figure 8. Figure 8a shows that the histogram of the Lena plain image has curved slanting bars. In contrast, Figure 8b shows that the histogram is a well-organized plain bar with uniform distribution. These well-organized plain bars provide great immunity against the histogram attack. This shows that the proposed scheme is efficient.

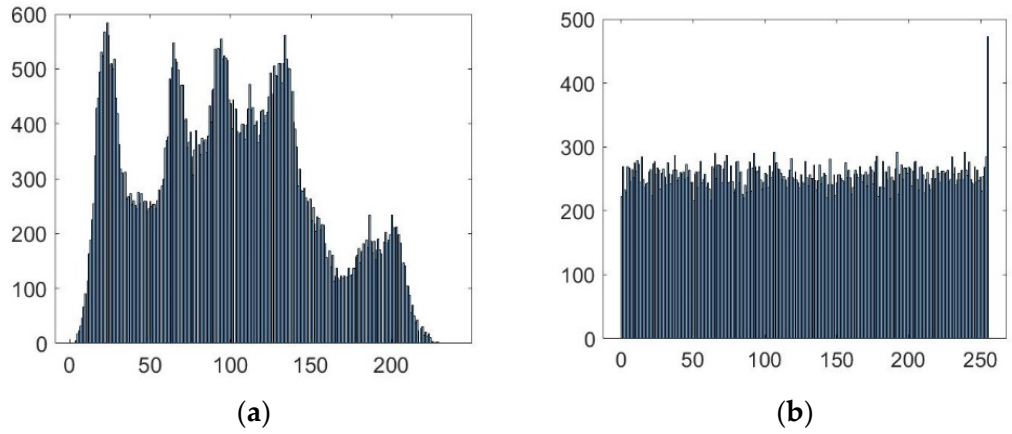


Figure 8. The Lena grayscale image histogram: (**a**) plain image; (**b**) encrypted image.

5.2.2. Analysis of the Correlation Coefficient

For any plain and natural images, the pixels are arranged in systematic ways. The close pixels are correlated in an intense manner. The correlation coefficient (*CC*) is another security parameter by which the inter-pixel correlation is found. These adjacent pixels are diagonally, vertically, or horizontally aligned to one another. Image ciphers are expected to disrupt these adjacent pixels. To analyze the *CC* of the proposed scheme, we took 3000 pairs of consecutive pixels from both the cipher and original images in an arbitrary way. *CC* was calculated using the following equation:

$$CC = \frac{A\sum_{l=1}^{A}(x_l \times y_l) - \sum_{l=1}^{A} x_l \times \sum_{l=1}^{A} y_l}{\sqrt{\left(A\sum_{l=1}^{A} x_l^2 - \left(\sum_{l=1}^{A} x_l{}^2\right)\right)\left(A\sum_{l=1}^{A} y_l^2 - \left(\sum_{l=1}^{A} y_l{}^2\right)\right)}} \quad (30)$$

Here, A denotes the number of pixels; the neighboring pixels are referred to by x and y. The correlation distribution for the adjacent pixels is shown in Figure 9.

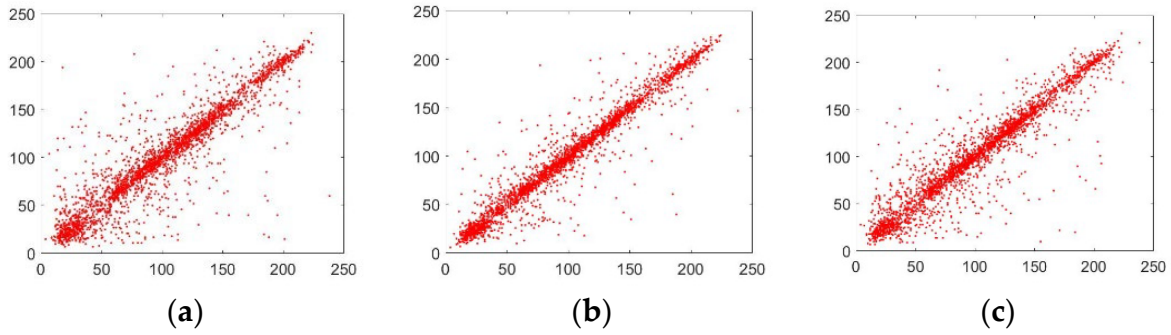


Figure 9. *Cont.*

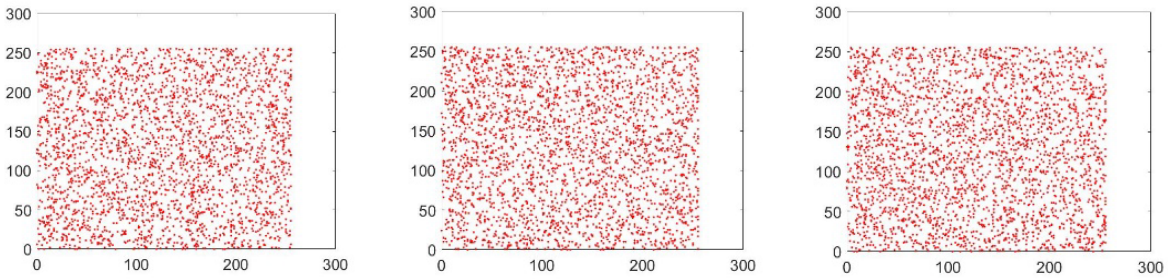


Figure 9. The adjacent pixel correlation distribution with directions: (**a**) horizontal component of the input Lena plain image; (**b**) vertical component of the input Lena plain image; (**c**) diagonal component of the input Lena plain image; (**d**) horizontal component of the generated Lena encrypted image; (**e**) vertical component of the generated Lena encrypted image; (**f**) diagonal component of the generated Lena encrypted image.

Figure 9 demonstrates that the cipher and plain images are extremely distinct from each other, asserting the success of the suggested image cipher.

5.3. Analysis of Information Entropy

The metric of information entropy (IE) could be used to judge the randomness and arbitrariness in some images. Shannon [55] in 1949 provided the concept of IE using the following mathematical equation:

$$E(k) = \sum_{i=0}^{2^n-1} d(k_i) log \frac{1}{d(k_i)} \tag{31}$$

where $E(k)$ is the IE of the information source k. The probability of k_i is represented by $d(k_i)$, and the number of the given image pixels is represented by n. Moreover, the largest value of this metric is calculated as 8 for any encrypted image with 256 grayscale values.

Table 2 demonstrate that the cipher and plain images are extremely distinct from each other, asserting the success of the suggested image cipher. It also observed that the cipher and plain images are extremely distinct from each other, asserting the success of the suggested image cipher.

Table 2. The comparison of the correlation coefficient(s) (*CC*) between our proposed image encryption scheme with other image encryption schemes.

Images	Encryption Algorithm	Correlation Direction		
		Horizontal	Vertical	Diagonal
Original Lena image	Our Algorithm	0.8941	0.9172	0.9516
Encrypted Lena image	Our Algorithm	0.0065	−0.0016	0.0063
Lena	[45]	−0.0164	−0.0083	0.0080
Lena	[51]	0.0038	0.0024	0.0052
Lena	[52]	0.0044	0.0151	0.0012
Lena	[53]	−0.0077	0.0117	0.0119
Peppers	[54]	0.0171	−0.0213	0.0118
MRI	[56]	0.0060	0.0123	0.0023
Lena	[57]	0.0038	−0.0011	0.0010

The results of IE of our proposed scheme are presented in Table 3. The calculated average IE for the encrypted images is 7.9955, which is near 8.

Table 3. The information entropy (IE) results analysis between our proposed image encryption scheme and other schemes.

Encryption Algorithm	Images	Size	Original	Encrypted
Our Algorithm	Lena	256 × 256	7.5690	7.9957
	Baboon	256 × 256	6.6962	7.9952
	Bridge	256 × 256	7.0097	7.9960
	Cameraman	256 × 256	6.4523	7.9952
	Airplane	256 × 256	6.2616	7.9954
	Clock	256 × 256	6.7057	7.9955
	Moon	256 × 256	7.1701	7.9956
	Ship	256 × 256	6.7093	7.9956
	Average	**256 × 256**	**6.8217**	**7.9955**
[40]	Lena	256 × 256	6.3872	7.9953
[45]	Lena	512 × 512	7.4456	7.9994
[51]	Lena	256 × 256	7.5683	7.9971
[52]	Lena	512 × 512	7.4456	7.9993
[53]	Lena	512 × 512	7.4456	7.9994

5.4. Plaintext Sensitivity Analysis (Differential Attack)

Cryptanalysts exhaust all possibilities to hack the hidden key of a security product. In this vast range of attacks, the differential attack is included. In the special attack dynamics, the cryptanalyst encrypts a plain image and obtains its encrypted version. Further, one more encrypted image is obtained after making a tiny alteration in the same input image by changing a single pixel value. The discovery of the confidential key can potentially be achieved by closely inspecting these two cipher images. In the literature, two validation metrics were employed to investigate the prowess and immunity of an encryption scheme for the images against differential attacks. These were the unified average changing intensity (*UACI*) and the 'number of pixels change rate' (*NPCR*). The following mathematical equations are used to find these two metrics.

$$NPCR = \frac{\sum_{a,b} D(a.b)}{C \times D} \times 100\% \tag{32}$$

Here, the dimensions of the images are denoted by C and D. Further, D(a, b) is defined as:

$$D(a,b) = \begin{cases} 1, if\ C(a,b) \neq C'(a,b), \\ 0, if\ C(a,b) = C'(a,b) \end{cases} \tag{33}$$

$$UACI = \frac{1}{C \times D}\left[\sum_{i,j} \frac{|C(a,b) - C'(a,b)|}{255}\right] \times 100\% \tag{34}$$

In these equations, C and C′ denote the encrypted images with a change in the pixel value and no change in the pixel value, respectively.

Table 4 shows the average values of NPCR and UACI for the chosen eight images, i.e., 99.6282 and 33.2459, respectively.

A comparison has also been made in Table 5. Additionally, Table 5 shows *CC* results between neighboring pixels for the input Lena plain image and its encrypted version. It is clear from Table 5 that the results approximate to one for the plain image and zero for the cipher image. Moreover, Table 5 presents a comparison of this security parameter between the published works and the proposed scheme. One can see that the results are comparable. The NPCR results of the proposed scheme are better than the ones in [40,45,51–54]. Moreover, the proposed cipher could only beat [53] regarding UACI.

Table 4. The calculated average values of NPCR and UACI for different images.

Images	NPCR	UACI
Lena	99.5743	33.0509
Baboon	99.6521	33.1627
Bridge	99.6506	33.3766
Cameraman	99.6445	33.6619
Airplane	99.6518	33.8155
Clock	99.6323	33.1338
Moon	99.6216	32.5399
Ship	99.5987	33.2262
Average	**99.6282**	**33.2459**

Table 5. The calculated average values of NPCR and UACI of our proposed scheme and its results comparisons with other existing encryption schemes.

Algorithm	Average NPCR	Average UACI
Ours	99.6282	33.2459
[40]	99.6091	33.4437
[45]	99.6000	33.4000
[51]	99.6000	33.4000
[52]	99.6200	33.4500
[53]	99.6100	33.4200
[54]	99.6110	33.2320

5.5. Peak Signal-to-Noise Ratio (PSNR) Analysis

The basic aim of any image encryption scheme is to cause a maximum difference between the plain image and its encrypted version. This metric is employed for this purpose by the cryptographers whose mathematical formula is

$$\begin{cases} PSNR = 20\, log_{10}\left(255/\sqrt{MSE}\right) dB \\ MSE = \frac{1}{A\times B}\sum_{k=1}^{A}\sum_{l=1}^{B}(P_0(k,l) - P_1(k,l))^2 \end{cases} \tag{35}$$

where A and B are the dimensions of the image. $P_0(k, l)$ and $P_1(k, l)$ refer to the intensity values of pixels of plain and cipher images. The mean squared error (MSE) is the error between the two images. $PSNR$ and MSE are inversely proportional to each other, as the equation implies. The higher the MSE value, the better the scheme will be. Analogously, a lower value of $PSNR$ is desirable.

Table 6 shows the $PSNR$ values for the plain, cipher, and decrypted images. The first row of this table has the entries of infinity (Inf) for (O–D). This indicates that plain and decrypted images are exactly the same. Further, this occurred due to the factor $MSE = 0$. This further implies that the proposed scheme is lossless. Moreover, the second row of Table 6 shows the values for (O–C), which are better than the ones given in [58–60]. These stats depict that the proposed scheme is better. A comparative analysis between the published works and the suggested scheme can be seen in Table 6. The IE of the Lena image and the mean values of all the chosen images of the suggested scheme are superior to the one in [39]. Hence, the suggested image cipher is immune to the entropy attack.

Table 6. The PSNR results between the plain, cipher, and decrypted images: 'O–C' stands for the original and cipher images, 'O–D' stands for the original and decrypted images.

Encryption Algorithm	PSNR	Lena	Baboon	Bridge	Cameraman	Airplane	Clock	Moon	Ship
Our algorithm	PSNR(O–D)	Inf	Inf	Inf	Inf	Inf	Inf	Inf	Inf
	PSNR(O–C)	8.5534	8.0991	8.3854	7.7515	9.9684	7.2682	9.3150	9.1370
[58]	PSNR(O–D)	96.2956							
	PSNR(O–C)	9.0348							
[59]	PSNR(O–C)	8.6878							
[60]	PSNR(O–C)	9.0486							

5.6. Noise and Data Loss Analysis

In a real-time scenario, the images are vulnerable to the assaults of data loss and noise. A good scheme is expected to successfully cope with them. Figure 10 shows the noise analysis. The pepper and salt noise was mixed with various densities of 0.1, 0.2, 0.3, and 0.4 in the cipher images of Lena, baboon, cameraman, and airplane (Figure 10a–d). The images restored after applying the decryption algorithm over them were redrawn in Figure 10e–h, respectively. Obviously, these decrypted images are still recognizable, which demonstrates that the suggested scheme can avert the noise attack. Similarly, a data loss analysis is demonstrated in Figure 11. Figure 11a–d represent the encrypted images with 0%, 25%, 50%, and 50% data losses in the encrypted images of Lena, Lena, airplane, and cameraman, respectively. The decrypted images are shown in Figure 11e–h. One can see that the plain images can be appreciated easily, implying that the proposed image cipher has the capability to foil data loss attacks.

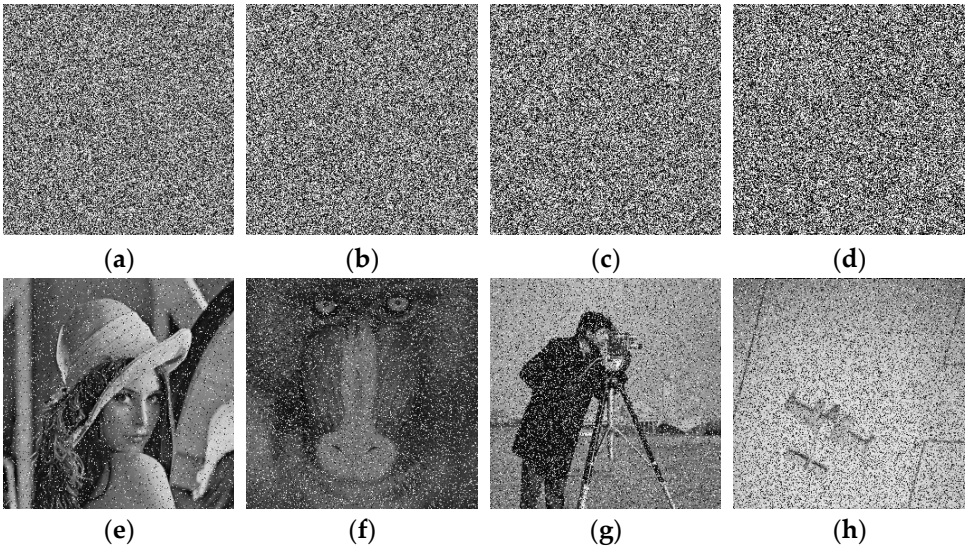


Figure 10. Pepper and salt noise attacks with different densities: (**a**) Lena cipher image by accumulating pepper and salt noise with noise density 0.1; (**b**) baboon cipher image by accumulating pepper and salt noise with noise density 0.2; (**c**) cameraman cipher image by accumulating pepper and salt noise with noise density 0.3; (**d**) airplane cipher image by accumulating pepper and salt noise with noise density 0.4; (**e**) the decrypted image obtained from (**a**); (**f**) the decrypted image obtained from (**b**); (**g**) the decrypted image obtained from (**c**); and (**h**) the decrypted image obtained from (**d**).

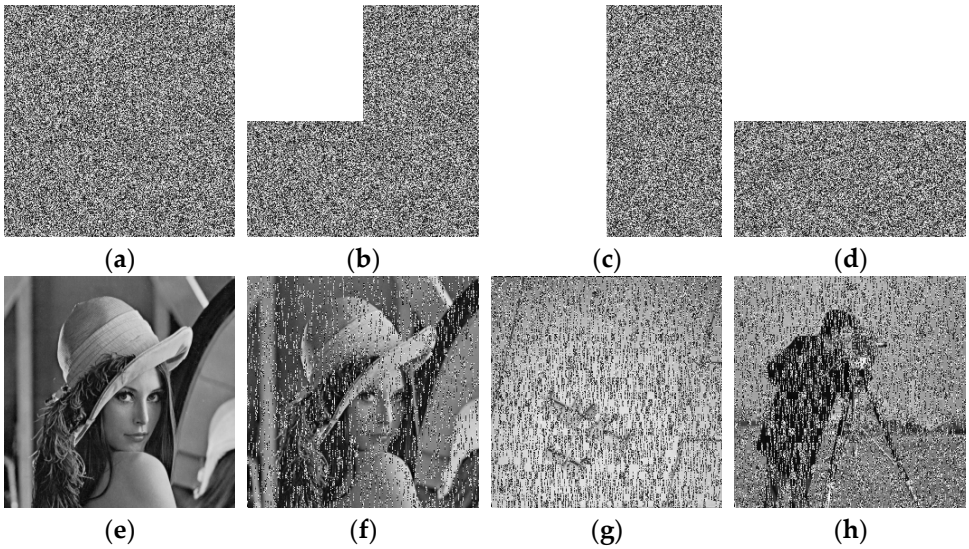


Figure 11. Analysis of the data loss attack: (**a**) 0% data loss in the encrypted image of Lena; (**b**) 25% data loss in the encrypted image of Lena; (**c**) 50% data loss in the encrypted image of the airplane; (**d**) 50% data loss in the encrypted cameraman image; (**e**) decrypted Lena image from the image drawn in (**a**); (**f**) decrypted Lena image from the image drawn in (**b**); (**g**) decrypted airplane image from the image drawn in (**c**); (**h**) decrypted cameraman image from the image drawn in (**d**).

5.7. Computational Time Analysis

Apart from security concerns, speedy ciphers are more demanding in this modern world. The proposed work was carried out using the system with the specification of Intel® Core™ i7-3740QM CUP@2.70 GHz, 8GB RAM. Further, the Windows 10 Education version operating system was used with MATLAB R2018a.

Table 7 shows the execution times for the encryption and decryption algorithms against the chosen images. Upon calculating the average values for encryption and decryption algorithms of the chosen images, we obtained 0.1830 and 0.1831 s. Moreover, the execution time was far better than the published works [40,61] because this scheme is based on the block-level swapping of pixels, due to which we gained a dramatic increase in computational time.

Table 7. Execution time of encryption (Enc) and decryption (Dec) in seconds.

Images	Enc	Dec
Lena	0.1842	0.1861
Baboon	0.1817	0.1879
Bridge	0.1869	0.1793
Cameraman	0.1842	0.1844
Airplane	0.1834	0.1834
Clock	0.1856	0.1870
Moon	0.1796	0.1839
Ship	0.1786	0.1733
Average	**0.1830**	**0.1831**
[40]	4.0200	-
[61]	1.4800	-

Apart from this, there is another associated concept called encryption throughput (*ET*). This refers to the dimensions of the image is encrypted/decrypted in some unit time. Its equation is

$$ET = \frac{Image_{Size}(Bite)}{Encryption_{Time}(Second)} \quad (36)$$

Table 8 demonstrates the encryption throughout the suggested scheme along with its comparison with other works. The results show that the proposed scheme vividly outperforms these works regarding the important metric of the *ET*.

Table 8. Suggested scheme's encryption throughout and a comparative analysis with other works.

Images	ET in Mbits
Lena	3.3488
Baboon	3.5257
Bridge	2.7833
Cameraman	2.8507
Airplane	3.3411
Clock	2.8292
Moon	3.4437
Ship	2.9401
Average	**3.1328**
[16]	0.4240
[40]	0.1419
[62]	2.3861

The time complexity calculation of the proposed algorithm is as follows. Step 6 of Section 3.1 takes O(3MN) to generate the three streams of random numbers of the chaotic map employed in this work. Now, we work on Section 3.2. Step 4.2 contributes O(2MN) to the complexity. Further, the time complexity for the swapping operations takes O(3MN). The simple assignment operation of Step 4.4 takes O(MN). Lastly, Step 5 for the XOR operation consumes O(MN). By adding all of these time complexities, we obtain O(10 MN) as the time complexity for the suggested cipher. This time complexity beats these studies [11,16,63], since the computational complexities of these studies are O(15 MN + $24\sqrt{\backslash MN}$), O(24 MN), and O(24 MN), respectively. The proposed cipher beats [11,16,63] by a factor of $\frac{24MN}{10MN} = 2.4$ (43).

$$\frac{15MN + 24\sqrt{MN}}{10MN} = \frac{15 \times 256 \times 256 + 24\sqrt{256 \times 256}}{10 \times 256 \times 256} \approx 1.505 \quad (37)$$

at $M = 256$ and $M = 256$. As the dimensions of the input images increase, this factor will also increase.

6. Conclusions

Upon surveying images from the literature cryptography, one will find that many schemes for image encryption have been written at different granularity levels. These include bits, pixels, DNA strands, and block-level. To expedite the speed, we proposed a new image encryption algorithm in this study. The underlying idea that differentiates it from the other works is that the whole block of pixels has been swapped with another block of pixels. This act gave competitive results as far as the speed and encryption throughput are concerned. The given image is reshaped into a linear array. Through the streams of random numbers, two blocks were selected, consisting of eight pixels. After selection, they were swapped with each other. This action was repeated for an arbitrary number of times. The scrambled image was further XORed with the last and third streams of chaotic data to obtain the final cipher image. The intertwining logistic map was employed in this work. The essential feature of plaintext sensitivity was realized by adding SHA-256 hash codes. An exhaustive security analysis and machine experiments vividly demonstrated the robust defiance of ubiquitous threats from the cryptanalysis community and the chances for real-world applications of the suggested image cipher. In particular, we gained encryption and decryption speeds of 0.1842 and 0.1861 s, respectively, which no doubt gave a major push to the state-of-the-art. In the future, we intend to inject the DNA strands to come up with more security and defiance to potential threats. Moreover, one limitation plagues the proposed cipher, i.e., the sides of the resolution of the given input image must be a multiple

of 8. In the future, we will extend our work so that it may cater to all dimensions of the given images.

Author Contributions: M.H. and N.I. collected the data from different resources; M.H., N.I. and M.A. performed the formal analysis and simulation; M.H., N.I. and F.U.R. contributed to the writing—original draft preparation; H.A.H., M.A.K. and S.A. conducted the writing—review and editing; C.Y.Y., M.A.K. and S.A. performed the supervision; T.M.G., M.H. and F.U.R. drafted the pictures and tables; C.Y.Y., T.M.G., M.A.K., M.A. and F.U.R. performed the revisions and improved the quality of the draft. 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: The simulation files/data used to support the findings of this study are available from the corresponding author upon request.

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

References

1. Bashir, Z.; Iqbal, N.; Hanif, M. A novel gray scale image encryption scheme based on pixels' swapping operations. *Multimed. Tools Appl.* **2020**, *80*, 1029–1054. [CrossRef]
2. Wan, Y.; Wang, S.; Du, B. A bit plane image encryption algorithm based on compound chaos. *Multimed. Tools Appl.* 2022, *in press*. [CrossRef]
3. Zheng, J.; Zeng, Q. An image encryption algorithm using a dynamic S-box and chaotic maps. *Appl. Intell.* 2022, *in press*. [CrossRef]
4. Sharkawy, N.H.; Afify, Y.M.; Gad, W.; Badr, N. Gray-Scale Image Encryption Using DNA Operations. *IEEE Access* **2022**, *10*, 63004–63019. [CrossRef]
5. 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]
6. Mirzaei, O.; Yaghoobi, M.; Irani, H. A new image encryption method: Parallel sub-image encryption with hyper chaos. *Nonlinear Dyn.* **2011**, *67*, 557–566. [CrossRef]
7. Patro, K.A.K.; Soni, A.; Netam, P.K.; Acharya, B. Multiple grayscale image encryption using cross-coupled chaotic maps. *J. Inf. Secur. Appl.* **2020**, *52*, 102470. [CrossRef]
8. Iqbal, N.; Abbas, S.; Khan, M.A.; Fatima, A.; Ahmed, A.; Anwer, N. Efficient image cipher based on the movement of king on the chessboard and chaotic system. *J. Electron. Imaging* **2020**, *29*, 023025. [CrossRef]
9. Girdhar, A.; Kapur, H.; Kumar, V. A novel grayscale image encryption approach based on chaotic maps and image blocks. *Appl. Phys. A* **2021**, *127*, 1–12. [CrossRef]
10. Chowdhary, C.L.; Patel, P.V.; Kathrotia, K.J.; Attique, M.; Perumal, K.; Ijaz, M.F. Analytical Study of Hybrid Techniques for Image Encryption and Decryption. *Sensors* **2020**, *20*, 5162. [CrossRef]
11. Hanif, M.; Abbas, S.; Khan, M.A.; Iqbal, N.; Rehman, Z.U.; Saeed, M.A.; Mohamed, E.M. A Novel and Efficient Multiple RGB Images Cipher Based on Chaotic System and Circular Shift Operations. *IEEE Access* **2020**, *8*, 146408–146427. [CrossRef]
12. Iqbal, N.; Hanif, M.; Abbas, S.; Khan, M.A.; Rehman, Z.U. Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding. *J. Inf. Secur. Appl.* **2021**, *58*, 102809. [CrossRef]
13. Xu, Q.; Sun, K.; Cao, C.; Zhu, C. A fast image encryption algorithm based on compressive sensing and hyperchaotic map. *Opt. Lasers Eng.* **2019**, *121*, 203–214. [CrossRef]
14. Hasheminejad, A.; Rostami, M. A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map. *Optik* **2019**, *184*, 205–213. [CrossRef]
15. Wu, T.; Xie, S.-C.; Zhang, J.-Z.; Zhao, H.-X. Color image encryption algorithm based on the position index and chaos theory. *J. Electron. Imaging* **2019**, *28*, 53008. [CrossRef]
16. Iqbal, N.; Abbas, S.; Khan, M.A.; Alyas, T.; Fatima, A.; Ahmad, A. An RGB Image Cipher Using Chaotic Systems, 15-Puzzle Problem and DNA Computing. *IEEE Access* **2019**, *7*, 174051–174071. [CrossRef]
17. Shao, Z.; Liu, X.; Yao, Q.; Qi, N.; Shang, Y.; Zhang, J. Multiple-image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyrator domain. *Signal Process. Image Commun.* **2019**, *80*, 115662. [CrossRef]
18. Girdhar, A.; Kumar, V. A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. *Multimed. Tools Appl.* **2018**, *77*, 27017–27039. [CrossRef]
19. Iqbal, N.; Hanif, M.; Abbas, S.; Khan, M.A.; Almotiri, S.H.; Al Ghamdi, M.A. DNA Strands Level Scrambling Based Color Image Encryption Scheme. *IEEE Access* **2020**, *8*, 178167–178182. [CrossRef]
20. Zhang, X.; Wang, X. Multiple-image encryption algorithm based on mixed image element and chaos. *Comput. Electr. Eng.* **2017**, *62*, 401–413. [CrossRef]

21. Chai, X.; Chen, Y.; Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.* **2017**, *88*, 197–213. [CrossRef]
22. Suri, S.; Vijay, R. A synchronous intertwining logistic map-DNA approach for color image encryption. *J. Ambient Intell. Humaniz. Comput.* **2018**, *10*, 2277–2290. [CrossRef]
23. Enayatifar, R.; Abdullah, A.H.; Isnin, I.F.; Altameem, A.; Lee, M. Image encryption using a synchronous permutation-diffusion technique. *Opt. Lasers Eng.* **2017**, *90*, 146–154. [CrossRef]
24. Cao, C.; Sun, K.; Liu, W. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. *Signal Process.* **2018**, *143*, 122–133. [CrossRef]
25. Patro, K.A.K.; Acharya, B. A novel multi-dimensional multiple image encryption technique. *Multimed. Tools Appl.* **2020**, *79*, 12959–12994. [CrossRef]
26. Wang, X.; Xu, D. A novel image encryption scheme using chaos and Langton's Ant cellular automaton. *Nonlinear Dyn.* **2014**, *79*, 2449–2456. [CrossRef]
27. Li, S.; Li, C.; Chen, G.; Zhang, D.; Bourbakis, N. A General Cryptanalysis of Permutation-Only Multimedia Encryption Algorithms. IACR's Cryptology ePrint Archive. 2015, pp. 1–20. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.449&rep=rep1&type=pdf (accessed on 2 January 2022).
28. Li, C.; Lo, K.-T. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Process.* **2011**, *91*, 949–954. [CrossRef]
29. Özkaynak, F.; Ozer, A.B. Cryptanalysis of a new image encryption algorithm based on chaos. *Optik* **2016**, *127*, 5190–5192. [CrossRef]
30. Zhang, W.; Wong, K.-W.; Yu, H.; Zhu, Z.-L. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 584–600. [CrossRef]
31. Zhang, W.; Yu, H.; Zhao, Y.-L.; Zhu, Z.-L. Image encryption based on three-dimensional bit matrix permutation. *Signal Process.* **2016**, *118*, 36–50. [CrossRef]
32. Hua, Z.; Zhou, Y.; Pun, C.-M.; Chen, C.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **2014**, *297*, 80–94. [CrossRef]
33. Chen, L.; Ma, B.; Zhao, X.; Wang, S. Differential cryptanalysis of a novel image encryption algorithm based on chaos and Line map. *Nonlinear Dyn.* **2016**, *87*, 1797–1807. [CrossRef]
34. Hoang, T.M.; Thanh, H.X. Cryptanalysis and security improvement for a symmetric color image encryption algorithm. *Optik* **2018**, *155*, 366–383. [CrossRef]
35. Wu, J.; Liao, X.; Yang, B. Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation. *Signal Process.* **2018**, *142*, 292–300. [CrossRef]
36. Zhou, Y.; Bao, L.; Chen, C.P. A new 1D chaotic system for image encryption. *Signal Process.* **2013**, *97*, 172–182. [CrossRef]
37. Khan, M. A novel image encryption scheme based on multiple chaotic S-boxes. *Nonlinear Dyn.* **2015**, *82*, 527–533. [CrossRef]
38. Patro, K.A.K.; Acharya, B. Secure multi–level permutation operation based multiple colour image encryption. *J. Inf. Secur. Appl.* **2018**, *40*, 111–133. [CrossRef]
39. Bano, A.; Singh, P. Image encryption using block based transformation algorithm. *Pharma Innov. J.* **2019**, *8*, 11–18.
40. Artiles, J.A.; Chaves, D.P.; Pimentel, C. Image encryption using block cipher and chaotic sequences. *Signal Process. Image Commun.* **2019**, *79*, 24–31. [CrossRef]
41. Liu, X.; Xiao, D.; Huang, W.; Liu, C. Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model. *IEEE Access* **2019**, *7*, 57188–57199. [CrossRef]
42. Ramasamy, P.; Ranganathan, V.; Kadry, S.; Damaševičius, R.; Blažauskas, T. An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map. *Entropy* **2019**, *21*, 656. [CrossRef]
43. Xu, L.; Gou, X.; Li, Z.; Li, J. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Opt. Lasers Eng.* **2017**, *91*, 41–52. [CrossRef]
44. Zhu, S.; Zhu, C. Plaintext-Related Image Encryption Algorithm Based on Block Structure and Five-Dimensional Chaotic Map. *IEEE Access* **2019**, *7*, 147106–147118. [CrossRef]
45. Chai, X.-L.; Gan, Z.; Zhang, M. A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. *Multimed. Tools Appl.* **2016**, *76*, 15561–15585. [CrossRef]
46. 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]
47. Ye, G. A block image encryption algorithm based on wave transmission and chaotic systems. *Nonlinear Dyn.* **2013**, *75*, 417–427. [CrossRef]
48. 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]
49. Khan, M.A.; Ahmad, J.; Javaid, Q.; Saqib, N.A. An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. *J. Mod. Opt.* **2017**, *64*, 531–540. [CrossRef]
50. IEEE Computer Society Standards Committee. *IEEE Standard for Binary Floating-Point Arithmetic*; IEEE: Piscataway, NJ, USA, 1985; Volume 754.

51. Ye, R.; Xi, Y.; Ma, Y. A chaotic image encryption scheme using swapping based confusion approach. In Proceedings of the 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), Wuhan, China, 13–15 October 2016; pp. 374–377. [CrossRef]
52. Fu, C.; Zhao, G.-Y.; Gao, M.; Ma, H.-F. A chaotic symmetric image cipher using a pixel-swapping based permutation. In Proceedings of the 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013), Xi'an, China, 22–25 October 2013; pp. 1–6. [CrossRef]
53. Chen, J.-X.; Zhu, Z.-L.; Fu, C.; Yu, H. An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism. *Opt. Express* **2013**, *21*, 27873–27890. [CrossRef]
54. Chen, J.-X.; Zhu, Z.-L.; Fu, C.; Yu, H. A fast image encryption scheme with a novel pixel swapping-based confusion approach. *Nonlinear Dyn.* **2014**, *77*, 1191–1207. [CrossRef]
55. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Technol. J.* **1949**, *28*, 656–715. [CrossRef]
56. Parvees, M.Y.M.; Samath, J.A.; Bose, B.P. Secured Medical Images—A Chaotic Pixel Scrambling Approach. *J. Med. Syst.* **2016**, *40*, 1–11. [CrossRef] [PubMed]
57. Wong, K.-W.; Kwok, B.S.-H.; Yuen, C.-H. An efficient diffusion approach for chaos-based image encryption. *Chaos Solitons Fractals* **2009**, *41*, 2652–2663. [CrossRef]
58. Zhu, C. A novel image encryption scheme based on improved hyperchaotic sequences. *Opt. Commun.* **2012**, *285*, 29–37. [CrossRef]
59. Norouzi, B.; Mirzakuchaki, S. A fast color image encryption algorithm based on hyper-chaotic systems. *Nonlinear Dyn.* **2014**, *78*, 995–1015. [CrossRef]
60. Taneja, N.; Raman, B.; Gupta, I. Combinational domain encryption for still visual data. *Multimed. Tools Appl.* **2011**, *59*, 775–793. [CrossRef]
61. Rehman, A.U.; Liao, X.; Kulsoom, A.; Ullah, S. A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps. *Multimed. Tools Appl.* **2015**, *75*, 11241–11266. [CrossRef]
62. Hu, T.; Liu, Y.; Gong, L.-H.; Guo, S.-F.; Yuan, H.-M. Chaotic image cryptosystem using DNA deletion and DNA insertion. *Signal Process.* **2017**, *134*, 234–243. [CrossRef]
63. Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **2018**, *155*, 44–62. [CrossRef]