applied sciences

MDPI

Article

A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information

Dani Elias Mfungo, Xianping Fu *, Yongjin Xian and Xingyuan Wang

School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China; danimfungo@dlmu.edu.cn (D.E.M.); matxyj@163.com (Y.X.)
* Correspondence: fxp@dlmu.edu.cn

Abstract: The complexity of chaotic systems, if used in information encryption, can determine the status of security. The paper proposes a novel image encryption scheme that uses chaotic maps and fuzzy numbers for the secure transmission of information. The encryption method combines logistic and sine maps to form the logistic sine map, as well as the fuzzy concept and the Hénon map to form the fuzzy Hénon map, in which these maps are used to generate secure secret keys, respectively. Additionally, a fuzzy triangular membership function is used to modify the initial conditions of the maps during the diffusion process. The encryption process involves scrambling the image pixels, summing adjacent row values, and XORing the result with randomly generated numbers from the chaotic maps. The proposed method is tested against various attacks, including statistical attack analysis, local entropy analysis, differential attack analysis, signal-to-noise ratio, signal-to-noise distortion ratio, mean error square, brute force attack analysis, and information entropy analysis, while the randomness number has been evaluated using the NIST test. This scheme also has a high key sensitivity, which means that a small change in the secret keys can result in a significant change in the encrypted image The results demonstrate the effectiveness of the proposed scheme in ensuring the secure transmission of information.

Keywords: image encryption; fuzzy logic; chaotic system; logistic map; sine map; Hénon map

Citation: Mfungo, D.E.; Fu, X.; Xian, Y.; Wang, X. A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information. *Appl. Sci.* **2023**, *13*, 7113. https://doi.org/10.3390/app13127113

Academic Editor: Silvia Liberata Ullo

Received: 19 April 2023
Revised: 4 June 2023
Accepted: 5 June 2023
Published: 14 June 2023

1. Introduction

The requirement to transmit data and information over networks has led to a growing concern among stakeholders regarding the need to maintain security. Various information centers, such as those dealing with health, military operations, education, e-commerce, and finance, share valuable information through networks. In order to secure this information, different approaches and methods have been developed by Böhme et al. [1]. Recently, using images as a means of transmitting data has become increasingly popular, as observed by Fu et al. [2]. The encryption of images has been found to be a secure and convenient method for transferring information over networks, and these observations align with the study conducted by Erkan et al. [3]. The encryption of images and text can differ due to several factors such as the size of the information, the correlation among pixels, and the information entropy. When it comes to encrypting text, traditional methods such as DES, Triple DES, and AES, as described by Barker and Mouha [4], and NIST [5] are widely used, while in case of image encryption, both chaos and non-chaos methods are utilized. According to Rivest [6] and Pathak et al. [7], the popular techniques in image encryption are cryptographic hash functions and visual cryptography. When these techniques are combined, they can result in a highly secure encryption method for protecting information transferred by image. The complexity of chaotic systems results in a higher level of security for information during encryption, as observed by Teng et al. [8]. Key attributes that must be considered while employing chaos for encryption include initial condition sensitivity, ergodicity, simplicity, and randomness. Different chaotic maps are used to archive this. The

sine map, Hénon map, and logistic map have been utilized to generate a random sequence of numbers in a chaotic system. These observations align with the studies conducted by Pathak et al. [7], Wang et al. [9], and Pareek [10], respectively. The logistic map is a one-dimensional discrete-time chaotic system, which can be adapted to two- or three-dimensional systems to deliver complex confusion. As Hua et al. [11] explain, the sine map is the most widely used and useful map in chaotic image encryption, similar to other maps such as logistics and tent maps.

Phatak and Rao [12] provide a comprehensive overview of the logistic map and offer detailed explanations on the impact of small variations in the parameter value. On the other hand, the Hénon map is a two-dimensional array exhibiting chaotic behavior similar to the logistic map. In 1976, it was discovered by Hénon [13] that the 2D Hénon equation is capable of producing deterministic chaos via the stretching and folding dynamics of chaotic systems. As described by Xiao et al. [14], an image encryption technique was developed by combining compressive sensing with a hyper chaotic system. Wang et al. designed a hybrid system utilizing logistic and sine maps, resulting in a broader range of chaos and improved ergodicity. This approach demonstrates promising results in image encryption and highlights the potential of hybrid chaotic systems in enhancing encryption techniques. In recent research, Zhang et al. [15] have explored the complexity of dynamic systems in generating chaos and have leveraged this understanding to develop an innovative and effective encryption method. Specifically, they investigated the spatiotemporal chaos of two-dimensional nonlinear coupled map lattices and combined this with genetic operations to create a secure encryption algorithm. This study demonstrates the practical application of a 2D chaotic system in the field of cryptography and highlights the potential for leveraging complex dynamic systems in the development of new encryption methods. A study conducted by Mfungo et al. [16] introduces a novel image encryption technique that integrates the Kronecker XOR product, Hill cipher, and sigmoid logistic map. This innovation serves as a means of securing the flow of information by safeguarding data and information from potential hacking during transmission or storage. The proposed algorithm has proven to be both secure and efficient in terms of performance and has demonstrated resistance to a variety of attacks.

Valandar et al. [17] support the idea that the use of fuzzy sets concepts in combination with dynamical systems can be explored in the realm of image encryption. The research conducted by Moysis et al. [18] confirms that the logistic map was successfully modified through the integration of triangular fuzzy numbers. This modification led to the emergence of complex chaos characterized by a higher Lyapunov exponent value compared to the conventional map. The proposed modification involves adding fuzzy numbers produced by a membership function to the logistic sine map parameters for the purpose of modification. This approach highlights the potential of integrating fuzzy sets in the development of encryption techniques and demonstrates the value of modifying established dynamical systems to enhance their security.

The integration of logistic, Hénon, and sine maps with fuzzy numbers is a relatively new area of research. Despite some prior research on this topic, the proposed study aims to explore this area further by combining all of these concepts. In this proposed study, the technique of shuffling and scrambling pixel values has been employed in order to achieve a more effective alteration of image pixels. The intermediary image is generated by the process of summing up pixel values from different rows and columns from a scrambled image to create a new value at a particular position. The triangular membership values obtained from the intermediary image after the diffusion process is used to modify the initial values of the logistic sine maps, as well as the initial parameter values of fuzzy Hénon map. The resulting sequence key from these maps is then XORed to create a new, secure, and random sequence of secret keys, which is used in an exclusive operation with the intermediary image. By using the triangular membership values to modify the initial values and parameters of the maps, the resulting encrypted image has a higher level of unpredictability and complexity, which enhances the security of the encryption process.

Contribution of the Study

- The use of the triangular membership values in this study enhances the unpredictability and complexity of the resulting encrypted image, which increases the security of the encryption process. This method enhances the randomness of the generated keys and makes it difficult for hackers to predict or crack the encryption code. This approach is an improvement over traditional encryption methods that rely on fixed values and can be easily cracked using brute force attacks.
- The system for image encryption employs the Hénon map and a triangular membership function to generate a sequence of random numbers that can be used as a key. The Hénon map provides a source of randomness, while the membership function adds variability to the sequence, making it harder to predict. The resulting key is therefore more secure and suitable for encryption purposes. By incorporating fuzzy logic, the system introduces an extra layer of complexity, making it even more difficult for attackers to decode.
- To further enhance the security of the encryption system, the scheme combines the logistic sine map with the fuzzy Hénon map to generate secret keys. The use of multiple mathematical concepts increases the space of possible secret keys, making the system more robust against sensitivity attacks. This innovative approach to encryption has the potential to revolutionize the field of data security and can be applied in various contexts where secure communication is essential. With its ability to generate complex and unpredictable keys, the system provides an effective solution to the challenge of secure image encryption.

In summary, this study's structure consists of several sections. The second section offers an overview of the essential concepts and background information required to understand the proposed image encryption method. The third section provides a detailed description and illustration of the encryption process and its implementation. The fourth section showcases the simulation results, analysis, and evaluation of the proposed encryption method, as well as a comparison with other studies. Finally, the study concludes with a summary of the findings in the last section.

2. Preliminaries

2.1. Chaotic Maps

The logistic map is a mathematical function classified as a quadratic map, renowned for its capacity to generate intricate chaotic behavior. By manipulating a single control parameter, the logistic map showcases a diverse range of dynamic phenomena, encompassing periodicity, bifurcations, and chaotic regimes. Phatak and Rao [12] extensively elaborate on these behaviors, providing a comprehensive explanation. In particular, the bifurcations of the logistic map become increasingly pronounced when the control parameter surpasses a critical value of 3.5. The logistic map is formally defined by Equation (1), which is a recursive equation that describes the evolution of a population over time.

$$x_{n+1} = r x_n (1 - x_n) \tag{1}$$

The control parameter $r > 0$ is called the "biotic potential", while x is the initial condition parameter. The dynamics of the logistic map are intricately tied to the value of the parameter r, giving rise to three distinct phenomena: when $r > 1$, the system gradually converges to the stable fixed point at 0; for values of $1 \leq r \leq 3$, the system undergoes a loss of stability at the previous fixed point and a new fixed point emerges at $x = \frac{1}{r}$; as r exceeds 3.5, an intriguing phenomenon called bifurcation unfolds, revealing a complex and fascinating diagram.

The Hénon map is a two-dimensional nonlinear map that exhibits chaotic behavior. It was introduced by Michel Hénon [19] in 1976 as a simplified model of the Poincare section of a dynamical system inspired by the Lorenz map. The Hénon map comprises two equations that are interrelated and describe the changes in the state variables. The

second equation represents a linear relationship with respect to the first state variable, whereas the first equation represents a quadratic relationship involving both state variables. It is demonstrated in Equation (2), which provides a clear depiction of the Hénon map's characteristics. The Hénon map is known for its sensitivity to initial conditions, which is a hallmark of chaotic systems. Despite its simplicity, the Hénon map has been applied to a wide range of fields, including physics, biology, and cryptography, modeling dynamical systems that exhibit chaotic behavior, such as fluid dynamics and celestial mechanics.

$$\begin{aligned} x_{n+1} &= 1 - a{x_n}^2 + by_n \\ y_{n+1} &= x_n \end{aligned} \tag{2}$$

The equation can also be written as defined by Equation (3):

$$x_{n+1} = 1 - a{x_n}^2 + bx_{n-1} \tag{3}$$

The parameters a and b are crucial to the behavior of the map, and by default, the value of parameter a is set to 1.4, while parameter b is set to 0.3. These two parameters play a vital role in determining the behavior of the map and can be adjusted to achieve different outcomes. According to the findings of Benedicks and Carleson [20], one of the defining characteristics of the Hénon map is the existence of a strange attractor, which is a fractal set that governs the long-term behavior of the system. The shape of the strange attractor is highly dependent on the parameters of the Hénon map, with different parameter values leading to distinct attractors [20]. It has also been used in cryptography as a basis for chaos-based encryption schemes. One of the objectives of this proposed study is to integrate the Hénon map and the fuzzy mathematics concept to create a highly chaotic system for image encryption called the fuzzy Hénon map. The map exhibits complex behavior that can be utilized for secure image encryption. By utilizing the properties of both concepts, the proposed encryption scheme aims to provide a high level of security for image data.

According to Sato et al. [21], the sine map is a one-dimensional, discrete-time dynamical system that belongs to the class of chaotic maps. The sine map function described in Equation (4) is a fundamental yet powerful tool that maps real numbers onto themselves. This simple, nonlinear function is defined using a trigonometric formulation, specifically involving the sine of the preceding state variable. By employing Equation (4), the system effectively incorporates the influence of the previous state variable in its dynamic evolution. The sine map is known for its sensitivity to initial conditions and its ability to generate complex, irregular behavior. It is often used as a testbed for studying the properties of chaotic systems, such as Lyapunov exponents and fractal dimensions.

$$x_{n+1} = k \sin(\pi \times x)\ x\ \in\ [0,\ 1],\ k > 0 \tag{4}$$

When the value of parameter k approaches 1, the sine map exhibits chaotic behavior, with the values of x_n appearing randomly as non-convergent and aperiodic when $x \in [0, 1]$ and $k \in (0, 1]$. The sensitivity of the system to the parameter k makes it a useful tool for generating chaotic behavior and has been applied to various fields, such as cryptography and secure communication. By adjusting the value of parameter k, the sine map can be used to generate random sequences that can be utilized for encryption purposes. Another objective of the proposed study is to integrate the logistic map and the sine map to form a hybrid map called the logistic sine map that generates a sequence of random numbers used as secret keys. The logistic sine map is intended to be utilized as a key during the image encryption process to enhance the security and confidentiality of the image data. The resulting hybrid map exhibits more complex and unpredictable behavior than either map alone, making it a more secure option for encryption.

2.2. Fuzzy Number

Fuzzy numbers are a type of mathematical concept used to represent uncertainty and imprecision in data. Sato et al. [22] suggest that unlike traditional numbers, fuzzy numbers are not precise values but rather a range of possible values. They are represented by a membership function that assigns a degree of membership to each element of the universe of discourse. The degree of membership ranges from 0 to 1, with 0 representing no membership and 1 representing full membership. According to Ross [23], fuzzy numbers have found application in numerous domains, including engineering, economics, and decision making. They serve as a valuable tool for modeling uncertainty, pattern recognition, weather control systems, computer vision, and addressing vagueness in real-world scenarios. In the field of image processing, fuzzy numbers have been utilized for encryption, segmentation, clustering, and image classification. They offer a means to express the level of confidence in a statement or describe the quality of a product or service.

In triangular fuzzy membership function, which is depicted in Equation (5), there are three parameters that used to control inputs: a as minimum value; c as maximum value; and b as a middle value which is located the peak of triangle, while a and c are located at the bottom side of a triangle, thus $a \leq b \leq c$.

$$f(x, a, b, c) = \max\left(\min\left(\frac{x-a}{b-a}, \frac{c-x}{c-b}\right), 0\right) \tag{5}$$

In this proposed technique, we have utilized the triangular membership function to create a hybrid of the Hénon map and triangular membership values called fuzzy Hénon map. This results in a complex and random sequence number which is utilized as a secret key during the encryption process. Furthermore, we have designed a hybrid of the sine map and logistic map (the logistic sine map) to generate additional random sequence numbers that are also used as secret keys. In both hybrid maps, the triangular membership function has been employed to generate parameters that are used to modify the initial keys of the map equations. This approach enables us to generate keys that are highly suitable for image encryption.

3. Proposed Scheme

A scanning and shuffling method is employed to encrypt a plain image. However, using a 1D logistic and sine map for encryption has limitations such as low complexity, small key space, and insecurity. To address this, Equations (1)–(3) are modified to produce Equations (13) and (14), which are used during the encryption process. The fuzzy mathematics concept is applied to generate values that manipulate initial keys in each iteration and produce new cipher images. By doing so, image security is improved and better at handling differential attacks.

3.1. Scrambling and Shuffling of Image Pixels

The rearranging, shuffling, and shifting operations in steps 1–3 of the proposed image encryption scheme are used to increase the complexity and randomness of the encryption process. The motivation behind these operations is to make it difficult for an attacker to decipher the encrypted image without knowledge of the secret keys. The scrambling of the image pixels in step 1 ensures that the image data are not in their original form, making it difficult for an attacker to recognize the image. The shuffling of the rows in step 2 and the shifting of the columns in step 3 further increase the complexity of the encryption process by introducing additional randomness. Without these operations, the algorithm may be less effective in ensuring secure transmission of information.

Step 1: Take a grayscale plain image β of size 256×256 and divide it into four different equal blocks of $\beta_1, \beta_2, \beta_3, \beta_4$ such that $(\beta_1, \beta_2, \beta_3, \beta_4) \in \beta$ and rearrange those blocks as in Figure 1.

Step 2: Each block is scrambled by sorting odd columns only and shift them to left side, odd rows and shift them to the top of the image; for example, as illustrated in Figure 2a,

the value 88 at position $(3,2)$ is shifted two positions right to $(3,5)$, as seen in Figure 2b, and in the final stage Figure 2c, it is shifted one position upwards to $(2,5)$. The process is shown in Algorithm 1.

Step 3: During this step, the transformation of image pixels occurs by taking each block and interchanging their position diagonally, as illustrated in Figure 3.

(**a**) Original image (**b**) Segmented image

Figure 1. Image Partition.

187	244	91	51	198	186	82	103
209	150	207	51	67	174	2	133
253	88	197	232	97	54	150	223
222	142	204	33	235	182	34	18
206	208	245	247	224	123	167	7
184	177	243	41	245	124	228	143
244	27	109	141	218	27	42	84
172	159	194	42	29	194	82	203

(**a**) Original matrix

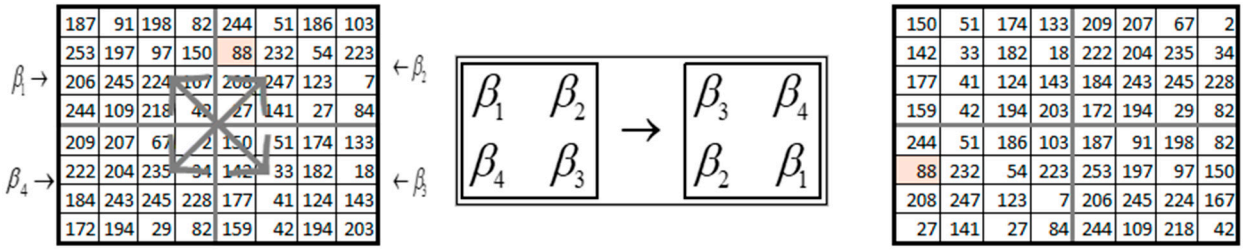
187	91	198	82	244	51	186	103
209	207	67	2	150	51	174	133
253	197	97	150	88	232	54	223
222	204	235	34	142	33	182	18
206	245	224	167	208	247	123	7
184	243	245	228	177	41	124	143
244	109	218	42	27	141	27	84
172	194	29	82	159	42	194	203

(**b**) Shift odd columns

187	91	198	82	244	51	186	103
253	197	97	150	88	232	54	223
206	245	224	167	208	247	123	7
244	109	218	42	27	141	27	84
209	207	67	2	150	51	174	133
222	204	235	34	142	33	182	18
184	243	245	228	177	41	124	143
172	194	29	82	159	42	194	203

(**c**) shift odd rows

Figure 2. Pixels rearrangement method 1.



(**a**) Image partition block (**b**) Block reshuffle

150	51	174	133	209	207	67	2
142	33	182	18	222	204	235	34
177	41	124	143	184	243	245	228
159	42	194	203	172	194	29	82
244	51	186	103	187	91	198	82
88	232	54	223	253	197	97	150
208	247	123	7	206	245	224	167
27	141	27	84	244	109	218	42

(**c**) New image block

Figure 3. Pixels rearrangement method 2.

Algorithm 1. The pseudo code of scrambling and shuffling image P

1. Start
2. Obtain plane image β of size $M \times N$
3. Convert β to decimal array of size $M \times N$
   - 3.1 Divide β into 4 equal blocks $\beta_1, \beta_2, \beta_3, \beta_4$
   - 3.2 In each block, shift the even column right and the odd rows upward.
   - 3.3 Reposition Blocks $\beta_3, \beta_4, \beta_2, \beta_1$
4. Combine Image Blocks and output new scrambled image β
5. Stop

3.2. Diffusion of Image Pixels

The process involved summing up the pixel values from different columns and rows to determine a new value at a specific position. Additionally, a triangular membership function derived from fuzzy mathematics was employed to obtain a manipulation key number. To achieve image diffusion, a hybrid random chaos system was created using three different chaotic maps, namely, the logistic map, the sine map, and the Hénon map.

Step 4: In this step, the manipulation is performed separately on each block, $\beta_1, \beta_2, \beta_3,$ and β_4. If e_i represents any column to be selected from a square matrix β, where $i \in [1-128]$, then $\beta(e_i)$ denotes the selection of a specific column in the matrix β. The summation of two-pixel values from different columns $\beta(e_i)$ and two adjacent pairwise rows is performed to derive a new value, as shown in Figure 4a–d, when Equation (6) is applied. For blocks β_1 *and* β_2, the value of $\beta(e_i)$ is 1, whereas for blocks β_3 and β_4, the value of $\beta(e_i)$ is 123. The process of summation is dependent on the number of iteration processes in each block, which can range from 1 to 4. However, for this study, only three iterations were conducted to increase performance. The top row remains unchanged, which simplifies the decryption process. The pseudo code algorithm of this process is shown in Algorithm 2.

$$\begin{cases} \beta(x_{i,j}) = \mathrm{mod}\left(\left(\beta(x_{i,j-1}) + \beta(x_{i-1,j})\right), 256\right) \\ x_{i,j} \leq 256 \leq 256n,\ n = 1, 2, 3, 4, \ldots\ldots n-1 \end{cases} \tag{6}$$

Step 5: Generation of fuzzy triangular membership for the k_m value. The functions described in Equation (7) refer to the membership values obtained from the image β^{xx}, which takes values in the interval [0, 1]. To obtain values close to 0.5, the value $\beta^{xx}(x_i)$ is adjusted piecewise, as shown in Equation (8). This facilitates the determination numbers between 0 and 1 of the sums of all membership values of the plain image and its mean, as illustrated in Equation (9). Here, n represents the total number of pixels in the image β^{xx}. Additionally, the k_m value is added to the initial keys of the fuzzy Hénon map and the logistic sine map as illustrated in next step.

$$\beta^{xx}(x_i) = \begin{cases} 0 & ;\quad x_i \leq a \ or \ x_i \geq c \\ \left(\frac{x_i - a}{b-a}\right) \times 255^{-1} & ; a \leq x_i \leq b \\ \left(\frac{c - x_i}{c-b}\right) \times 255^{-1} & ; b \leq x_i \leq c \end{cases} \tag{7}$$

$$MK = \begin{cases} 2 \times (\beta^{xx}(x_i))^2; \ \beta^{xx}(x_i) \leq 0.5 \\ 1 - (1 - \beta^{xx}(x_i))^2 \ ; \ \beta^{xx}(x_i) > 0.5 \end{cases} \tag{8}$$

$$k_m = \left(\sum_{i=1}^{n} MK_i + \sum_{i=1}^{n} \frac{MK_i}{n} \right) - floor\left(\sum_{i=1}^{n} MK_i + \sum_{i=1}^{n} \frac{MK_i}{n} \right) \tag{9}$$

Step 6: Generate Cipher K_1. The initial parameter is adjusted through the utilization of Equation (10). and subsequently integrated into the hybrid chaotic equation of the logistic sine map, as depicted in Equation (11). This incorporation facilitates the generation of a secret cipher key, K_1, as illustrated in Equation (12). The values of $x_{initial}$, $y_{initial}$,α, a, b, c, d, e are -1.2, 1.5, 2.1, 0.5, -0.65, and -0.7, respectively.

$$x_{initial} = (x_0 + k_m) - floor(x_0 + k_m) \tag{10}$$

$$\begin{gathered} w_{new} = \alpha \sin(\pi b(y_{initial} + a) x_{initial}(1 - x_{initial})) + d \\ v_{new} = \alpha \sin(\pi w_{new}(w_{new} + c) y_{initial}(1 - y_{initial})) + e \\ w_{values}(n+1) = w_{new} \end{gathered} \tag{11}$$

$$K_1 = w_{values} - floor(w_{values}/y) \times y \tag{12}$$

Given that $y = 1$ to ensures that the result of the operation is always between 0 and y and w_{values} is the array of w values, n is the index of the last element in the array and w_{new}

is the new w value to be added to the end of the array. Algorithm 3 shows the algorithm for generating secret keys k_1.

Step 7: Generate Cipher K_2. The initial value of the parameter $t = 0.0018901$ is adjusted using Equation (13) and incorporated into a hybrid of the Hénon map and the triangular membership function to be used as the initial parameter, x, in Equation (14). The values from β^{xx} are converted to membership values, as in Equation (16) with the left edge a_l, peak c_p and right edge b_r of the triangle as parameters, and used to find the centroid value C as in Equation (15). Then, the minimum and maximum possible values of C with respect to β^{xx} are found and normalize the value of C to the range [0, 0.5] using Equation (16). The resulting value of C represents the normalized crisp value that best represents the input values according to the triangular membership function, and it falls within the desired range. Based on Equation (17), the value of C is then applied to the fuzzy Hénon map. The secret key k_2 is obtained by finding the range of numbers between 0 and y, as shown in Equation (18). The initial value for $c = 0.0124$, $a_1 = 10$, $c_p = 100$, $b_r = 200$, $a = 1.4$, and $b = 0.2$, respectively.

$$x(1) = (t_0 + k_m) - floor(t_0 + k_m) \tag{13}$$

$$mem = trimf\left(\beta^{xx},\ [a_l,\ \mathrm{c}_p,\ \mathrm{b}_r]\right); \tag{14}$$

$$C = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} mem_{i,j} \times {\beta^{xx}}_{i,j}}{\sum_{i=1}^{m}\sum_{j=1}^{n} mem_{i,j}} \tag{15}$$

$$\begin{gathered} C_{min} = min(min(double(\beta^{xx}))); \\ C_{max} = max(max(double(\beta^{xx}))); \\ c = 0.5 \times ((C - C_{min})/(C_{max} - C_{min})); \end{gathered} \tag{16}$$

$$\begin{cases} x_i = 1 - (a \times x_{i-1}^2) + y_{i-1} \\ y_i = (b \times x_i) + c \end{cases} \tag{17}$$

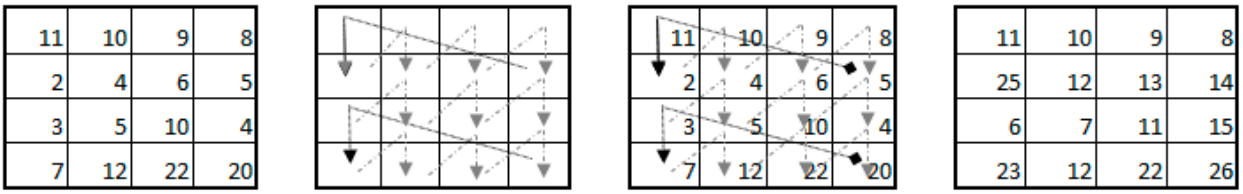
$$K_2 = y - floor(y) \tag{18}$$

Algorithm 4 shows the algorithm for generating the randomly sequenced set of secret keys from fuzzy numbers and the Hénon map.

Step 8: Cipher image C Based on Equation (19), the final step involves conducting an exclusive operation between β'', K_1 and K_2 to obtain the encrypted image, C. Exclusive operation is used in this step because it transforms intermediary ciphertext into final ciphertext by combining it with a secret key, which makes it difficult for unauthorized users to decrypt the data. The resulting final Ciphertext (C) is the exclusive operation of the intermediary ciphertext and the secret keys from the logistic sine map and the fuzzy Hénon map.

$$C = \beta^{xx} \oplus K_1 \oplus K_2 \tag{19}$$

The flowchart of how the encryption process is shown Figure 5. The decryption process of this scheme is the inverse of the encryption process from step 8 to step 1 above.



(**a**) Original matrix (**b**) Arrow direction (**c**) Pixel involves (**d**) New pixel values

Figure 4. Value manipulation.

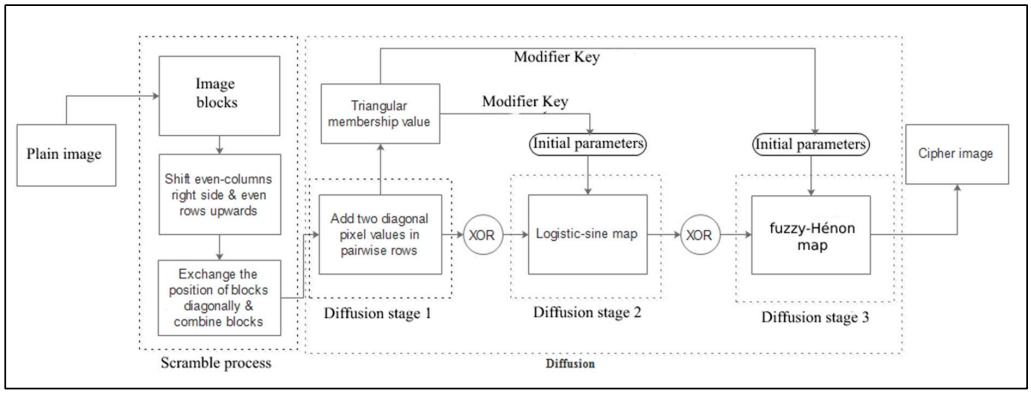


Figure 5. Flow diagram of proposed encryption mechanism.

Algorithm 2. The image pixel manipulation

1. Start
2. Input scrambled image β of size $M \times N$
3. Select any Column $\beta(e)$ from each block of size $\frac{N}{2}$; $N \in (1-256)$
4. Adding two diagonal pixel values in pairwise rows
   - 4.1 $for\ i = 1 : M \times N$
   - 4.2 $for\ j = 1 : M \times N$
   - 4.3 $\beta^x \leftarrow mod(\beta^x(i, j-1) + \beta^x(i-1, j), 256)$
   - 4.4 end
   - 4.5 end
5. $n \leftarrow \text{length}(\beta^x)$
6. Repeat Step 4, four times
7. Combine all the blocks
   - 7.1 $\beta^{xx} \leftarrow [\beta_4, \beta_3, \beta_2, \beta_1]$
8. Display β''
9. Stop

Algorithm 3. Generate cipher key K_1

1. Input: $x_0,\ k_m,\ \alpha,\ a,\ b,\ c,\ d,\ e$
2. Output: K_1
3. $x\_initial = \left(x_{(0)} + k_m\right) - floor\left(x_{(0)} + k_m\right)$
4. $w\_new = \alpha \times sin(\pi \times b \times (y\_initial + a) \times x\_initial \times (1 - x\_initial)) + d$
5. $v\_new = \alpha \times sin(\pi \times w\_new \times (w\_new + c) \times y\_initial \times (1 - y\_initial)) + e$
6. $w\_values[n+1] = w\_new$
7. $K_1 = w\_values - floor(w\_values)$

Algorithm 4. Generate cipher key K_2

1. Input: $t_0,\ k_m,\ \beta, a_l,\ c_p,\ b_r,\ a,\ b,\ c$
2. Output: K_2
3. $x[1] = (t_0 + k_m) - floor(t_0 + k_m)$
4. $mem = trimf\left(\beta^{xx},\ [a_l,\ c_p,\ b_r]\right)$
5. $C = sum(sum(mem \times \beta^{xx}))/sum(sum(mem))$
6. $C\_min = min(min(double(\beta^{xx})))$
7. $C\_max = max(max(double(\beta^{xx})))$
8. $C = 0.5 \times ((C - C\_min)/(C\_max - C\_min))$
9. $for\ i = 2$ to n
   - 9.1 $x[i] = 1 - a \times x[i-1]^2 + y[i-1]$
   - 9.2 $y[i] = b \times x[i] + C$
10. end
11. $K_2 = y - floor(y)$

3.3. Decryption Process

The decryption process is an essential component of the overall encryption scheme as it enables the recovery of the original data by reversing the operations performed during encryption. It is acknowledged that certain operations, such as modulo operations, may inherently possess irreversibility. However, within our proposed encryption scheme, these operations are strategically employed in a manner that ensures the feasibility of the decryption process. For instance, the modulo operation utilized in step 4 serves the purpose of constraining the result of the summation operation within a specific range. Although it introduces a level of non-invertibility, it does not impede the decryption process from being successfully executed. The carefully designed application of irreversible operations within our encryption scheme strikes a balance between security and practicality, allowing for a robust decryption process while maintaining the necessary security measures. The following are the steps for the decryption process.

Step 1: perform an exclusive operation between the final image C and K_1 to obtain an intermediary image of logistic sine map β^x to obtain C';

Step 2: perform an exclusive operation between secret keys from the fuzzy Hénon map K_2 and C' to obtain intermediary image β^{xx};

Step 3: divide the intermediary image β^{xx} into four equal blocks $\beta_1, \beta_2, \beta_3$ and β_4;

Step 4: reshuffle the position of each block diagonally between β_1 and β_3, as well as β_2 and β_4;

Step 4: subtract two diagonal pixel values in paired wise rows, means select two adjacent rows in an image, and subtract the pixel values diagonally across from each other, performing three iterations in each block;

Step 5: shift even columns to the left-side and even rows downwards in each block;

Step 6: reshuffle the position of each block diagonally between β_1 and β_3, as well as β_2 and β_4;

Step 7: combine the blocks to obtain the original image β.

4. Simulation Results and Security Evaluation

4.1. Experimental Setup

The reliability and validation of this proposed scheme was conducted on MATLAB R2016a with Processor Intel(R) Pentium(R) and with CPU N4200 @1.10GHz of system type 64-bit OS, $\times$64 based processor, 4.0 GB Random Access Memory, and 300 hard disks with the Windows 10 professional operating system. The standard gray-level images with sizes of 256 $\times$ 256 were used in this study, as shown in Figure 6.

The encryption and decryption process shown in Figure 7 managed to achieve the objectives of the study by developing the cryptography mechanism to protect the images.

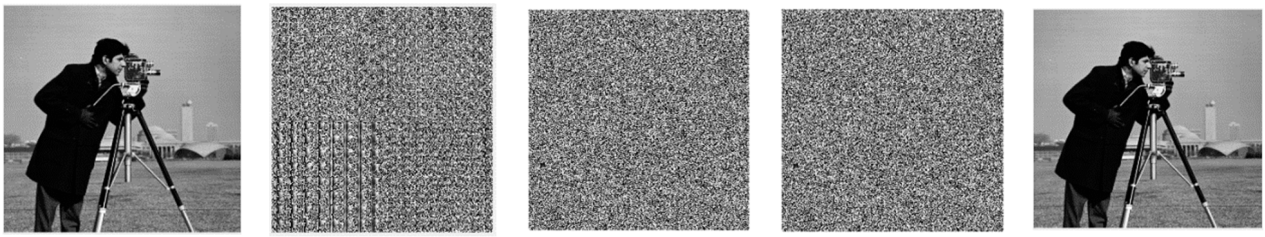
4.2. Variation Characteristics of Nonlinear Terms of the New System

When Equation (17) is used with different values of C from the triangular membership function, it forms different bifurcation diagrams, as seen Figure 8. The Lyapunov diagram is shown in Figure 9. Figure 10 shows both the bifurcation diagram and its Lyapunov exponent of the hybrid of logistic sine map as used in Equation (11).

In Equation (11), we have set the unknown parameter alpha (α) to a value of -1.2 and selected $(-1.9, 0.49995)$ as the initial value. Figure 11a presents the chaotic attractor diagram of the system. To examine the system's sensitivity to the initial value, we have compared the sequence diagrams with two different initial values: $(-1.85, 0.55)$ and $(-1.9, 0.49995)$. Figure 11b illustrates how minor changes in initial values affect the dynamic behavior of the system defined in (11). The chaotic properties of the system have significantly altered, which implies that the system is highly dependent on the initial value.

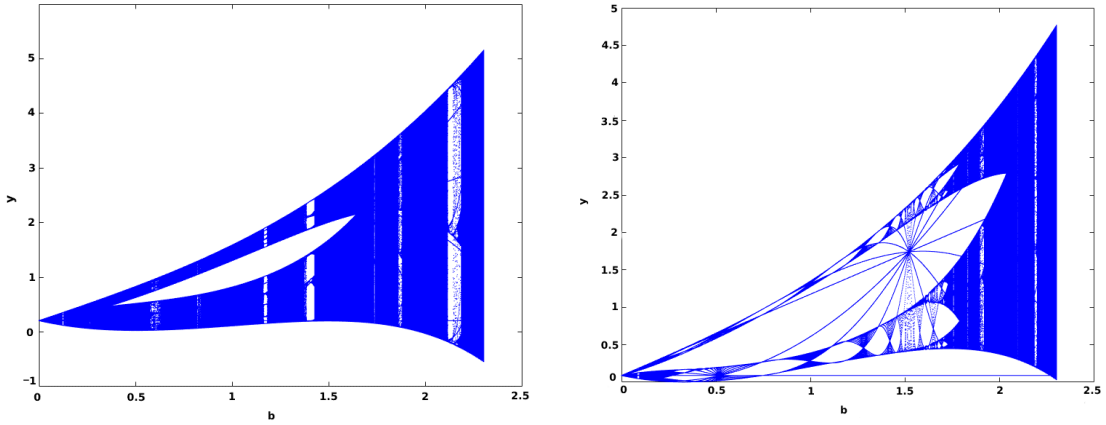
(**a**) Lena (**b**) Pepper (**c**) Cameraman (**d**) Rice (**e**) House

Figure 6. Images used for experiments.



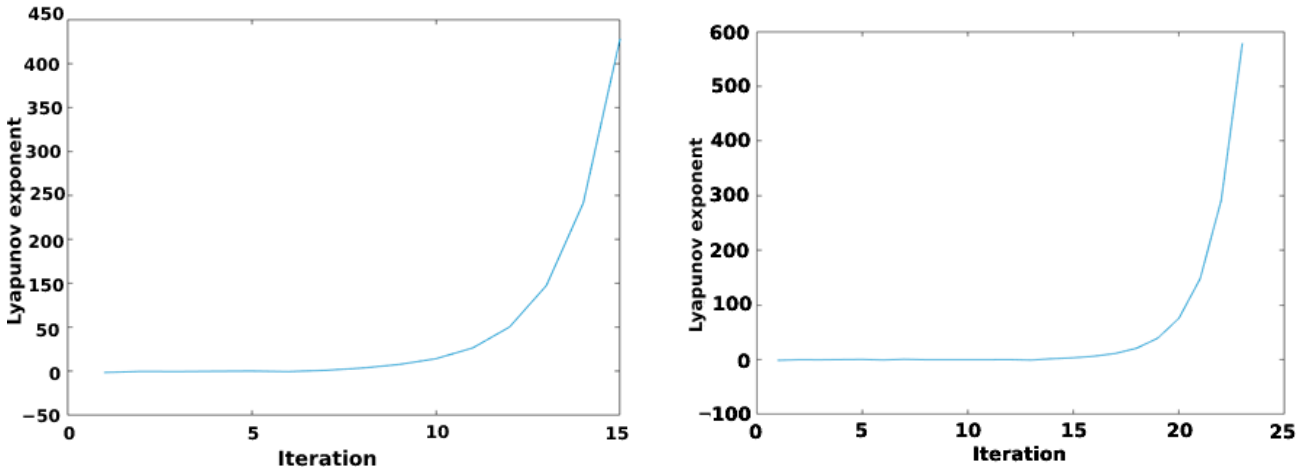
(**a**) Original image (**b**) Diffusion stage 1 (**c**) Diffusion stage 2 (**d**) Diffusion stage 3 (**e**) Decrypted image

Figure 7. The encryption and decryption process.



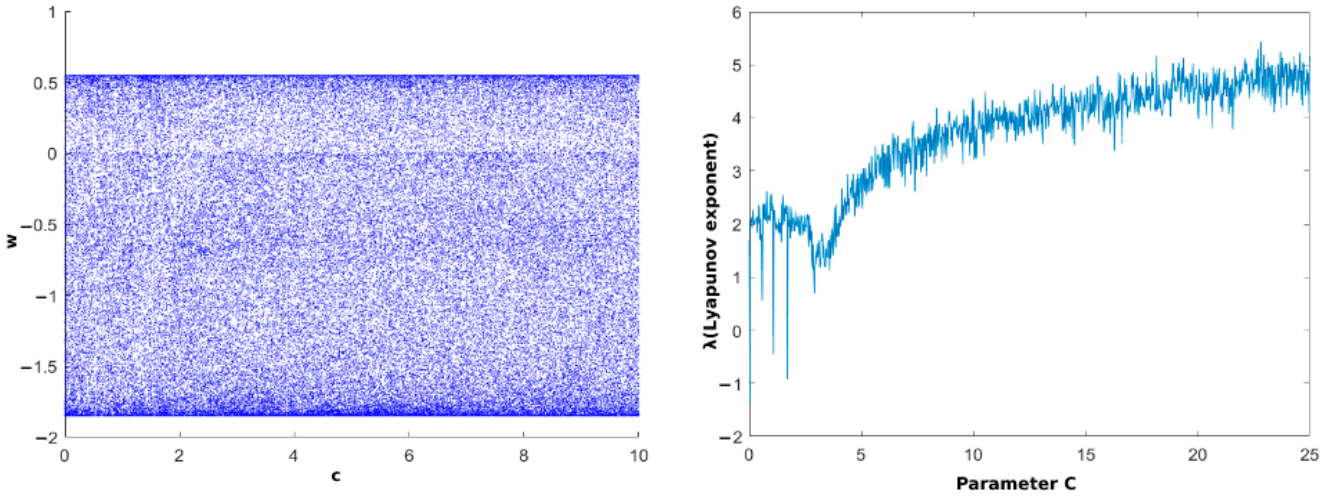
(**a**) Bifurcation with c = 0.2074 (**b**) Bifurcation with c = 0.089362

Figure 8. The bifurcation diagram of fuzzy Hénon map.



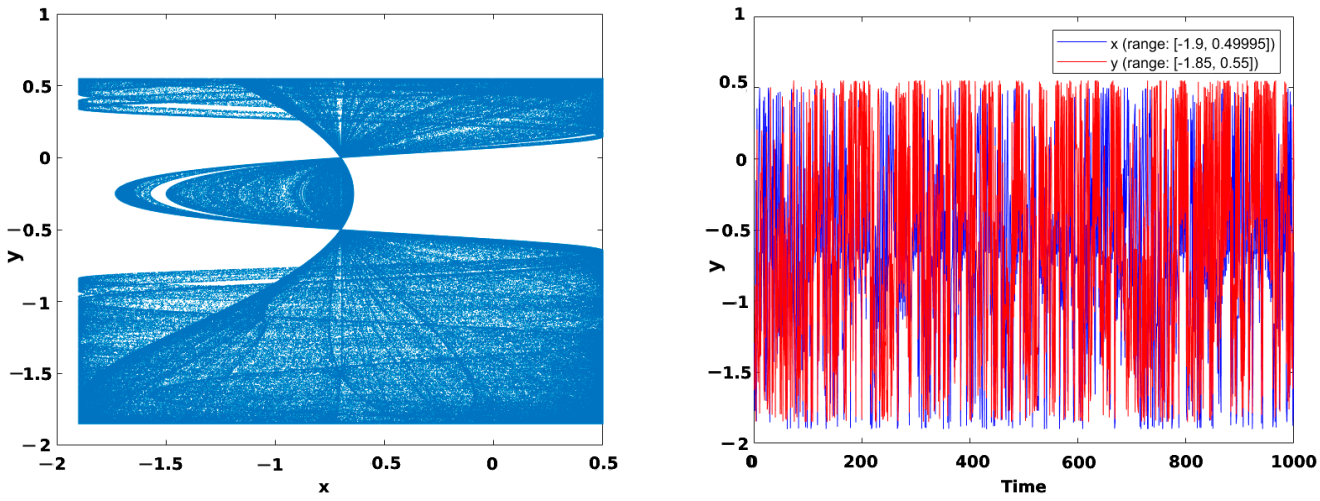
(**a**) LE with c = 0.2074 (**b**) LE with c = 0.089362

Figure 9. The Lyapunov exponent of fuzzy Hénon map.



(**a**) Bifurcation of logistic sine map (**b**) LE of logistic sine map

Figure 10. Logistic sine map: (**a**) the bifurcation diagram of the logistic sine map; (**b**) the Lyapunov exponent diagram of the logistic sine map.



(**a**) With alpha = −1.2, the attractor diagram with the initial value of (−1.9, 0.49995) (**b**) Time series comparison diagram with initial values of (−1.85, 0.55) and (−1.9, 0.49995)

Figure 11. Attractor diagram and time series diagram.

4.3. NIST Test

According to The National Institute of Standards and Technology (NIST) test [24], their chart sheet can be used to precisely assess how random a given test is. In our analysis of chaotic sequences produced by the chaotic hybrid map, we rely on 15 different random test methodologies from the NIST test, which is widely regarded as the gold standard for evaluating the quality of cryptographic algorithms. Achieving a *p*-value greater than 0.0001 is the basis of our success criteria because it is strong evidence that the sequence being generated by the 2D hybrid map is genuinely chaotic. The precision and comprehensiveness of the NIST test make it an essential tool for assessing the reliability and randomness of data, making it a key component of our proposed study. Table 1 shows the NIST randomness of 15 elements as used to indicate the *p*-value of the Cameraman encrypted image and comparisons with another study.

Table 1. NIST Test.

No	Test Name	*p*-Value	Results	Nardo et al. [25]	Results
1	Universal	0.2429	Pass	0.304126	Pass
2	Frequency	0.7985	Pass	0.883171	Pass
3	Block Frequency	0.2375	Pass	0.236810	Pass
4	Cumulative sums forward	0.9876	Pass	0.437274	Pass
5	Cumulative sums reverse	0.7654	Pass	0.437274	Pass
6	Runs	0.8529	Pass	0.759756	Pass
7	Longest run	0.2147	Pass	0.759756	Pass
8	Rank	0.1756	Pass	0.145326	Pass
9	FFT	0.6563	Pass	0.719747	Pass
10	Overlapping template	0.5644	Pass	0.595549	Pass
11	Approximate entropy	0.9343	Pass	0.867692	Pass
12	Serial	0.2231	Pass	0.554420	Pass
13	Linear Complexity	0.5281	Pass	0.534146	Pass
14	Random excursions	0.3541	Pass	0.494392	Pass
15	Random excursions variant	0.2781	Pass	0.236810	Pass

4.4. Statistical Attack

Security of the data depends on the states they are in, i.e., they can be data in motion, data at rest, or data in use. Most organizations prefer to transfer information in these states but mostly do so through insecure channels. Therefore, to maintain data security, a good and measurable mechanism must be established. The two mechanisms used to measure statistical attacks are the histogram and correlation coefficient analyses.

4.4.1. Analysis of Correlation Coefficients

The statistical method used to assess the magnitude and direction of the relationship between two variables is referred to as the correlation through bivariate analysis. The correlation coefficient value ranges between −1 and +1 and indicates the strength of the association between the two variables. When the correlation coefficient approaches 0, it signifies a weaker relationship between the variables. A positive (+) sign indicates a positive relationship, while a negative (−) sign indicates a negative relationship. An effective image encryption scheme should produce a randomly distributed output with minimal correlation between adjacent pixels. Typically, the correlation of pixels in both plain and cipher images is evaluated in the horizontal, vertical, and diagonal directions. The correlation coefficient r_{xy} between the adjacent pixels is defined and measured in Equation (20):

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

where

$$\operatorname{var}(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)^2\right),\ \operatorname{cov}(\mathrm{x},\mathrm{y}) = \mathrm{E}([x - E(X)][y - E(Y)]), E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i.$$

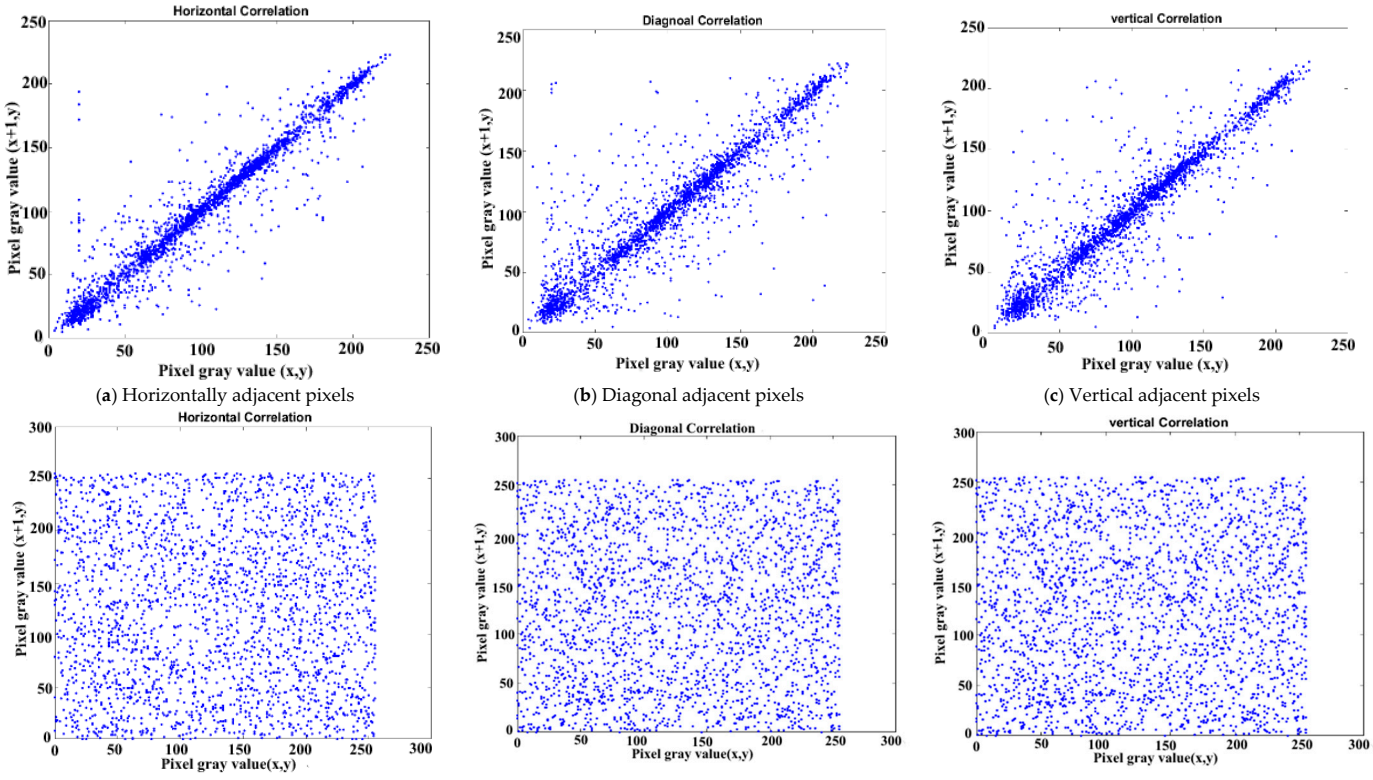
Here,x_i and y_i represent the gray level value of two adjacent pixels, where by $E(X)$ represents the mean of x_i and $E(Y)$ is the mean of y_i. After implementing Equation (20) in the proposed scheme, we noted a significant difference between the original and encrypted images. Table 2 displays the correlation coefficient between the two sets of images, while Table 3 compares the proposed scheme's results to other similar studies. These findings demonstrate that the proposed scheme exhibits superior resistance to statistical attacks. Figure 12 illustrates the random distribution of both the original and encrypted Baboon images.

Table 2. Relationships among variables before and after encryption.

Name	Original Image			Encrypted Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9410	0.9143	0.9647	0.00553	−0.00768	−0.00578
Cameraman	0.9335	0.9084	0.9591	0.0070	−0.0050	−0.0146
Peppers	0.9696	0.9434	0.9733	0.0004	−0.0018	−0.0063
Rice	0.9262	0.8979	0.9434	0.0021	0.0020	−0.0054

Table 3. Comparison of correlation coefficients.

Algorithm	Image	Horizontal	Vertical	Diagonal
	Plain Lena	0.9410	0.9143	0.9647
Proposed	Encrypted	0.0055	−0.0078	−0.0058
Zhu et al. [26]		0.0150	0.0044	−0.0036
Wang et al. [27]		0.0019	0.0038	−0.0019
Ramasamy et al. [28]		−0.0237	−0.0237	−0.0283
	Plain Pepper	0.9696	0.9434	0.9733
Proposed	Encrypted Pepper	0.0004	−0.0063	−0.0018
Ramasamy et al. [28]		−0.0727	−0.0225	−0.0242
Wu et al. [29]		0.0016	0.0059	0.0034
	Cameraman	0.9335	0.9084	0.9591
Proposed	Encrypted	0.0070	−0.0146	−0.0050
Wu et al. [29]		0.0024	0.0013	0.0098



(**a**) Horizontally adjacent pixels (**b**) Diagonal adjacent pixels (**c**) Vertical adjacent pixels

(**d**) Horizontally adjacent pixels of encrypted image (**e**) Diagonal adjacent pixels of encrypted image (**f**) Vertical adjacent pixels of encrypted image

Figure 12. Correlation of adjacent pixels in the plain Baboon image and the cipher Baboon image.

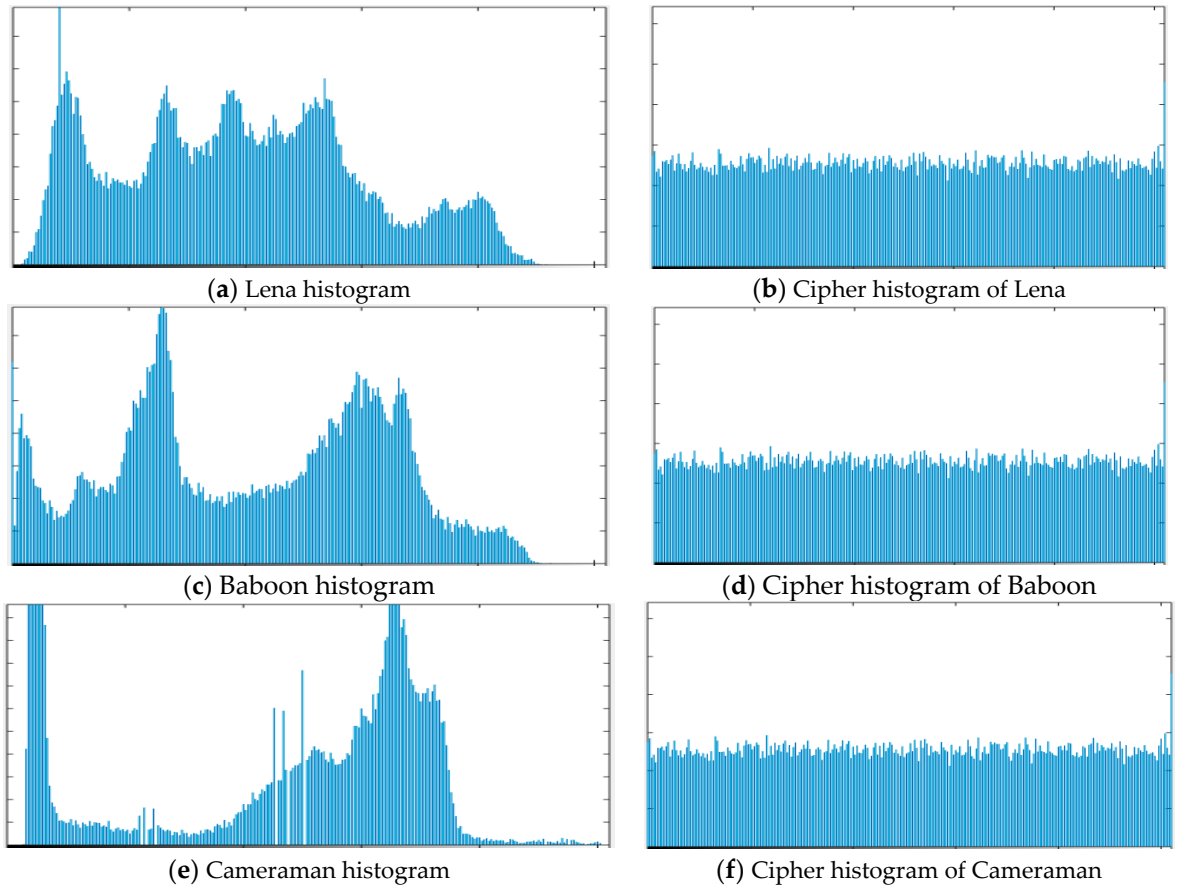
4.4.2. Histogram Analysis

An image histogram is a useful tool with which to visualize the statistical properties of an image based on the distribution of pixel values. Histogram shapes include the normal distribution, skewed distribution, double-peaked distribution, plateau distribution, flat

distribution, and edge peak distribution. A flat histogram is indicative of a secure and well-encrypted image technique. Figure 13 illustrates the histograms for the Lena, Baboon, and Pepper images for both the plain and encrypted versions. The flatness of the encrypted image histogram can be evaluated by determining its variance; this is conducted based on Equation (21) for an image of size $m \times n$:

$$Variance(h) = \frac{1}{2 \times n^2} \times \sum_{i=1}^{n} \sum_{j=1}^{m} (x_i - x_j)^2 \quad (21)$$

where h is the histogram vector value and x denotes the number of gray pixel values at (i, j) Table 4 displays the variance values for both the plain and encrypted images utilized in the experiments. A variance range averaging at 5000 indicates a more even distribution of pixel values, thus indicating a superior encryption mechanism.



(**a**) Lena histogram (**b**) Cipher histogram of Lena

(**c**) Baboon histogram (**d**) Cipher histogram of Baboon

(**e**) Cameraman histogram (**f**) Cipher histogram of Cameraman

Figure 13. Histogram for both plain images and encrypted images.

Table 4. Variance of images.

	Cameraman	Lena	Pepper	Rice	House
Original	3886.6300	2785.4833	3238.600	1805.6977	2118.0286
Encrypted	5671.4695	5698.5852	5672.7690	5600.6353	5764.8519

4.5. Differential Attack

In accordance with the findings reported by Wang et al. [27], even a minor modification in the pixel values of a plain image can lead to a substantial transformation in the resulting cipher image, thereby highlighting the efficacy of the encryption method. To quantitatively assess this effect, the normalized pixel change rate (NPCR) and the unified average change intensity (UACI) metrics are employed. NPCR, calculated using Equation (22), and UACI,

determined through Equation (23), mathematically capture the extent of change in pixel values between the plain and encrypted images:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\beta(i,j)}{M \times N} \times 100\% \quad (22)$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} e_1(i,j) + e_2(i,j)}{255 \times M \times N} \times 100\% \quad (23)$$

where

$$\beta(i,j) = \begin{cases} 0 if e_1(i,j) = e_2(i,j) \\ 1 if e_1(i,j) \neq e_2(i,j) \end{cases}$$

$M \times N$ represent the size of image β, and the cipher images e_1 and e_2 have one-pixel difference on their plaintext when encrypted with the same key. It is essential to ensure that any image encryption technique is secure and reliable, regardless of the size of the image being encrypted. To achieve this, the UACI (unified average changing intensity) and NPCR (number of pixel changing rate) values must meet certain critical values. Based on industry standards and best practices as stated by Wu and Agaian [30], the ideal value for UACI in an encrypted image is greater than 33%, while the ideal value for NPCR is greater than 99%. These critical values have been determined through rigorous analysis and testing and are considered to be the minimum requirement for ensuring the security and confidentiality of the encrypted image. Therefore, it is of utmost importance that the UACI and NPCR values meet these critical values in order to consider an image encryption technique secure. When these values are achieved, we can be confident that the encryption process has met its critical value and can be deemed secure. Hence, it is crucial to prioritize these values when evaluating and selecting image encryption techniques to ensure the confidentiality and security of sensitive images. Table 5 provides the NPCR and UACI value for images of size 256×256 which has been used in this study. Table 6 provides a comparison of the UACI and NPCR values obtained from this study with those of other similar studies. The findings demonstrate that the proposed method is suitable for the encryption process, even when there is a minor alteration of the pixel values in the images.

Table 5. Information global entropy, NPCR, and UACI.

	Information Entropy	NPCR %	UACI %
Lena	7.9968	99.6399	33.4308
Cameraman	7.9974	99.5773	33.3542
Pepper	7.9969	99.6094	33.5607
House	7.9972	99.6017	33.3707

Table 6. Information global entropy, UACI, and NPCR comparison.

Image	Proposed Entropy	Proposed NPCR	Proposed UACI	Enayatifar et al. [31] Info. Entropy	Enayatifar et al. [31] NPCR	Enayatifar et al. [31] UACI
Lena	7.9968	99.6399	33.4308	7.9975	99.5193	33.581
Cameraman	7.9974	99.5773	33.3542	7.9939	99.0039	33.102
Pepper	7.9969	99.6094	33.5607	7.9958	98.4972	32.940
House	7.9972	99.6017	33.3707	-	-	-

4.6. Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Distortion Ratio (SNR), and Mean Square Error Analysis

In the study conducted by Srivastava and Singh [32], the authors mention that the mean square error (MSE) and peak signal-to-noise ratio (PSNR) are commonly utilized to assess and evaluate the quality of images. The MSE is employed to measure the similarity

between encrypted images and plain images; a high-quality image is characterized by a low value of mean squared error (MSE), while a poor-quality image is indicated by a high MSE value. Equation (24) illustrates the computation of MSE by subtracting the cipher image from the original image. Conversely, a low value peak signal-to-noise ratio (PSNR) signifies the effectiveness of an image encryption technique. Equation (25) provides the calculation for PSNR in this context.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (P(i,j) - E(i,j))^2 \tag{24}$$

$$PSNR = 10 \times \log_{10} \frac{M \times N}{\sqrt{MSE}} \tag{25}$$

Here, $P(i,j)$ and $E(i,j)$ represent the pixels of the original and encrypted images, respectively. When $P(i,j) = E(i,j)$, the MSE value is always zero. Table 7 presents the results of the experiments conducted on encrypted images in terms of both the PSNR and MSE values, and demonstrates a high value of the MSE and a low value of the PSNR, which indicates good encryption technique. Moreover, the lower value of SNR indicates that the encrypted image has more noise, thus hindering the attacker's attempt to obtain information to a greater degree compared to less noise.

Table 7. MSE, PSNR, and SNR.

	Cameraman	Lena	Pepper	Rice	House
MSE	107.136	88.5046	93.44519	100.1538	131. 523
PSNR	8.3611	8.5085	8.4240	9.3281	9.2477
SNR	2.7773	1.2926	1.7061	2.7145	4.3285

4.7. Brute Force Attack

4.7.1. Key Sensitivity Analysis

Yavuz et al. [33] and Hua et al. [11] have demonstrated that the key sensitivity of a system becomes evident when even a minor alteration in parameters leads to a significant and distinct outcome. This can be conducted during encryption and decryption processes. Table 8 shows the correction coefficient when there is a slight change in parameter values during the encryption process: Round 1, $x_0 = 0.189 + 10^{-10}$, $a = 1.4$, $b = 0.3$; Round 2, $x_0 = 0.189 - 10^{-10}$, $a = 1.4$,$b = 0.3$; Round 3, $x_0 = 0.189$, $a = 1.4 + 10^{-10}$, $b = 0.3$; and Round 4, $x_0 = 0.189$, $a = 1.4$, $b = 0.3 + 10^{-10}$. While the correlations between the encrypted and original images are close to zero, the significant difference between their averages in all rounds indicates that the cipher images are indeed different. Figure 14 visually demonstrates the magnitude of difference in the resulting outcome when even slight changes occur in the parameters.

4.7.2. Secret Key Space Analysis

The control parameters of the sine, logistic, and Hénon maps are crucial in determining the level of security provided by the encryption mechanism. As the number of keys utilized in the encryption process increases, it becomes increasingly difficult for potential attackers to break the security measures. In this study, a total of three different keys were utilized; these secret keys are k_m obtained from the fuzzy number, k_1 obtained from the hybrid map of the logistic and sine maps, and k_2 obtained from the hybrid of the triangular membership function and the Hénon map. Ideally, key space used in encryption should be larger than 2^{100} [34] to handle brute force attack. According to the IEEE [34] standard, the precision number of floating points is 10^{15}. As part of this experiment, where three floating-point keys are utilized, the total number of key spaces can be approximated using Equation (26).

This equation serves as a crucial tool in estimating the size of the key space. This increased key space is better for resistance against brute-force attacks.

$$\text{Keys} = \left(10^{15\times 3}\right) \approx 2^{149} \tag{26}$$

Table 8. Key sensitivity analysis for cipher Lena.

Round	Small Change in Parameter Value	Average Correlation Coefficients
1	$x_0 = 0.189 + 10^{-10}$, $a = 1.4$, $b = 0.3$	−0.003030
2	$x_0 = 0.189 - 10^{-10}$, $a = 1.4$, $b = 0.3$	−0.005816
3	$x_0 = 0.189$, $a = 1.4 + 10^{-10}$, $b = 0.3$	−0.0000415
4	$x_0 = 0.189$,$a = 1.4$, $b = 0.3 + 10^{-10}$	−0.002644

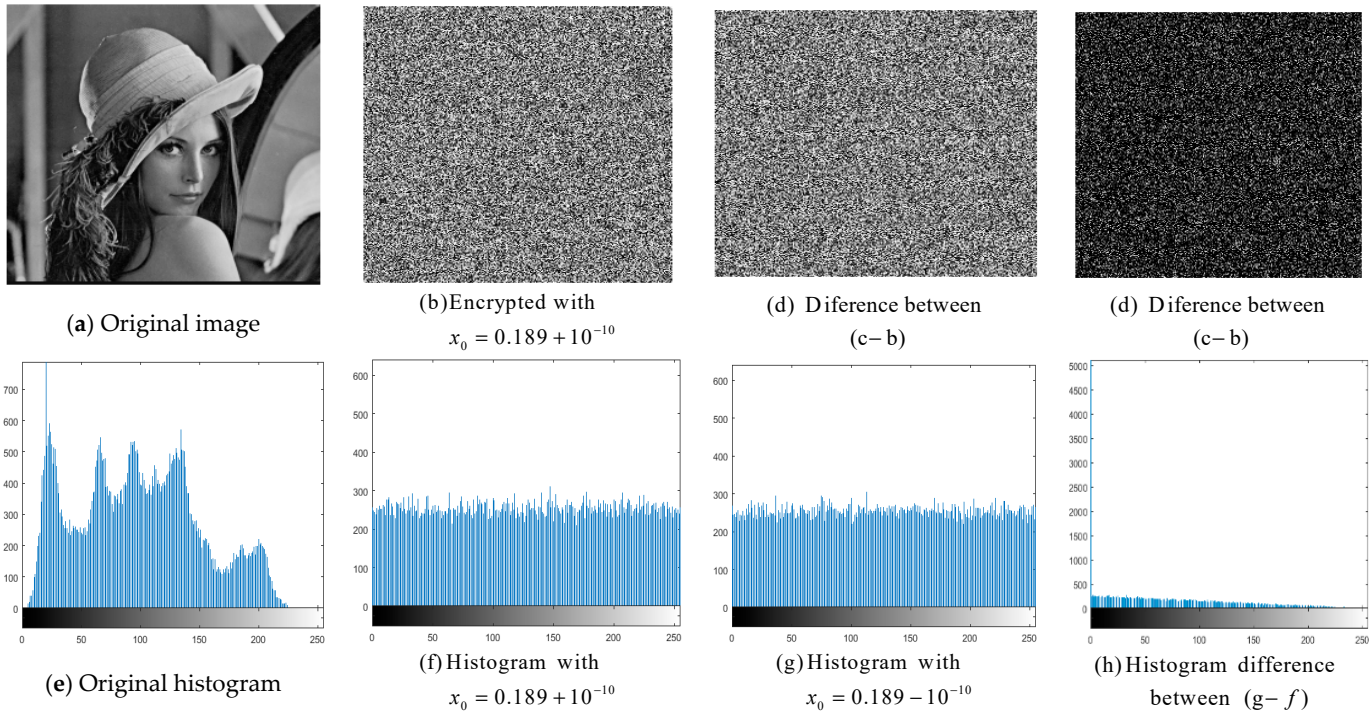


Figure 14. Key sensitivity analysis in Lena encryption image.

4.8. Entropy Analysis (Randomness Test)

4.8.1. Global Entropy Analysis

Ramasamy et al. [28] have provided evidence supporting the use of information entropy as a measure to evaluate the uncertainty or randomness of a variable in an image. The calculation of information entropy is performed using Equation (27), which is an essential component in quantifying the uncertainty of a given system. In this equation, parameter B represents the probability of pixel X within the image under consideration. By incorporating Equation (27) into our analysis, we gain valuable insights into the information content and distribution of the image's pixels. A high value of entropy indicates a good and strong encryption mechanism when $E \approx 8$. Table 5 shows the entropy values of both plain and encrypted images, while Table 6 provides a comparison with other studies. The results show that our proposed algorithm is suitable and less prone to revealing information, making it safe from brute force attacks.

$$E = \sum_{i=1}^{256} p(i) \times \log\left(\frac{1}{p(i)}\right) \tag{27}$$

4.8.2. Local Entropy Analysis

Local entropy is an important aspect of image encryption as it measures the amount of uncertainty or randomness within a small region of an image. By analyzing the local entropy of an image, as suggest by Wu et al. [35], it is possible to determine the degree of complexity and randomness present in the image, which can be indicative of its security against various attacks. To improve the security of image encryption schemes, it is necessary to consider the local entropy of the image and find ways to increase it. This can be achieved through various techniques, such as the use of more complex and diverse chaotic maps, the incorporation of additional randomness in the encryption process, and the application of various transformations to the image. Table 9 shows the local entropy of both plain and encrypted images used in this study.

Table 9. Local entropy of plain and encrypted images.

	Lena	**Rice**	**Cameraman**	**Pepper**	**House**
Local entropy of plain image	7.4710	6.9472	6.8835	7.4924	6.3964
Local entropy of encrypted image	7.8982	7.8988	7.8990	7.8973	7.8981

4.9. Speed Performance Test

In our study, we conducted a speed test on encrypted images with a size of 256 × 256, similar to the approach taken by Yavuz [36]. We compared our results with those obtained in other relevant studies. Our proposed encryption method not only demonstrated its robustness but also proved to be lightweight and highly efficient in terms of performance. Based on our findings, as shown in Table 10, we believe that the proposed encryption method offers an excellent solution for secure and quick encryption.

Table 10. Speed performance test.

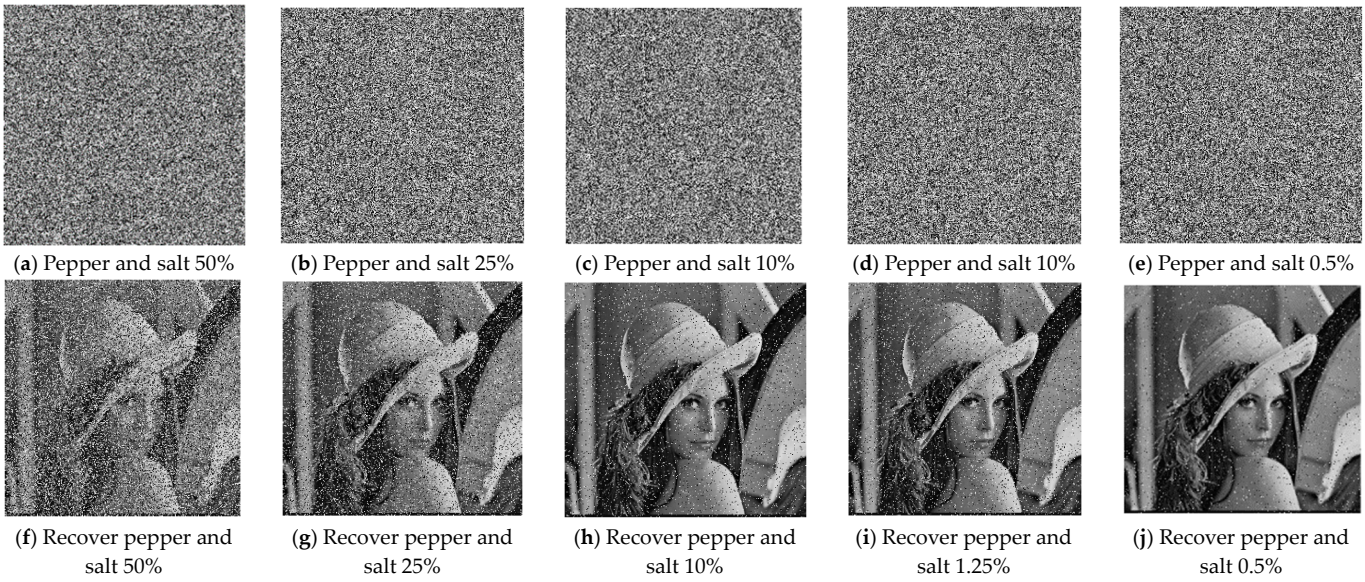
Algorithm	**Encryption Time**
Proposed	0.030
Yavuz et al. [33]	0.032
Wang and Yang [37]	0.19102
Gao et al. [38]	0.606

4.10. Noise and Data Loss Analysis

Our proposed encryption system has demonstrated superior performance when it comes to dealing with cipher data contamination that includes both data loss and noise. To test this, we applied 50%, 25%, 10%, 1.25%, and 0.5% noise to an encrypted Lena image and attempted to recover the original image. Our encryption system performed exceptionally well in the recovery process, highlighting its effectiveness in preserving the integrity and quality of encrypted data even in the presence of noise and data loss of less than 50%. We also tested our proposed encryption approach on encrypted images that experienced data loss, with the aim of recovering the original images. The test was conducted to measure data loss at different rates: 50%, 30%, 20%, and 10%.. Through our testing, we found that our encryption system was effective in reconstructing the original images from the cipher data, even when the encrypted images had experienced data loss of less than 30%. This underscores the robustness and reliability of our proposed encryption approach, which can be valuable in situations where the encrypted data are vulnerable to loss or corruption. See Figure 15 for noise effects and Figure 16 for data loss.

The reason for conducting noise tests in our proposed encryption process lies in the inherent stability provided by the utilization of chaotic maps and fuzzy numbers. These elements contribute to a high level of randomness and complexity within the encryption process. Chaotic maps, being dynamic systems, exhibit a sensitive dependence on initial conditions, resulting in significant output variations from even minor changes in the initial conditions. Fuzzy numbers, on the other hand, introduce the capability to accommodate

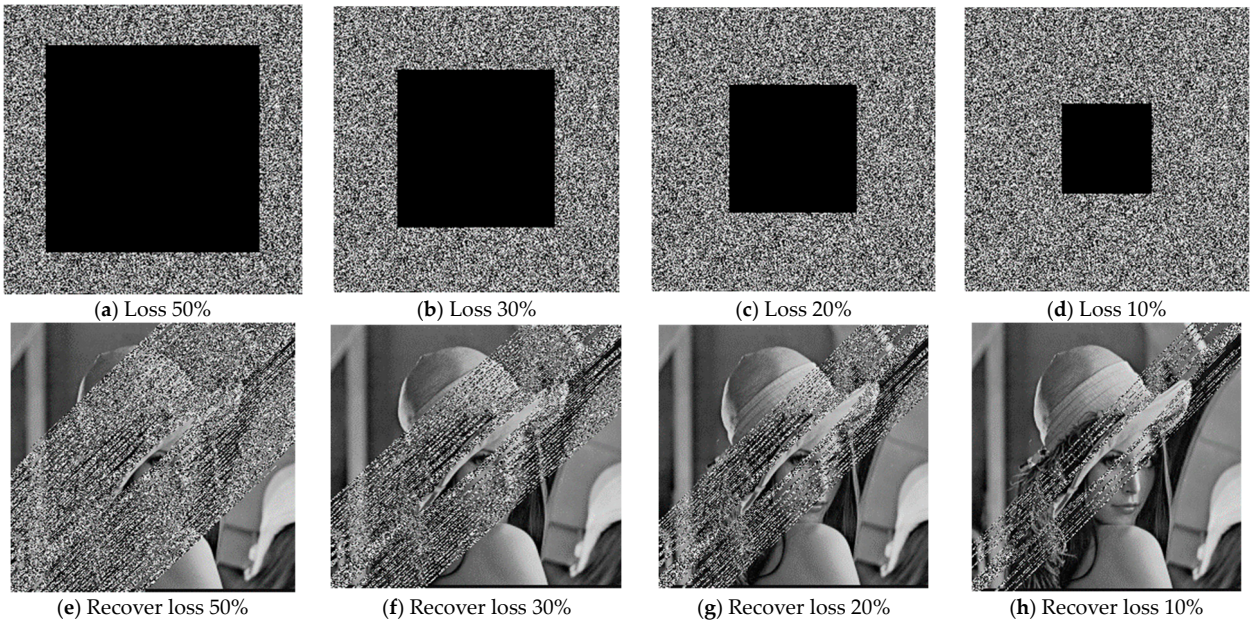
uncertainty and imprecision. By incorporating both chaotic maps and fuzzy numbers, our encryption scheme generates a highly intricate and random sequence of numbers, thereby impeding attackers seeing to decipher the encrypted data. Additionally, the chaotic nature of the encryption process enhances its resistance to noise and other forms of interference. Even small alterations in the input data will lead to substantial changes in the encrypted output, reinforcing the scheme's resilience against noise. In conclusion, the integration of chaotic maps and fuzzy numbers in our proposed encryption scheme introduces an additional layer of randomness and complexity, making it more challenging for attackers to decrypt the data while bolstering resistance against noise and interference during the decryption process.



(**a**) Pepper and salt 50% (**b**) Pepper and salt 25% (**c**) Pepper and salt 10% (**d**) Pepper and salt 10% (**e**) Pepper and salt 0.5%

(**f**) Recover pepper and salt 50% (**g**) Recover pepper and salt 25% (**h**) Recover pepper and salt 10% (**i**) Recover pepper and salt 1.25% (**j**) Recover pepper and salt 0.5%

Figure 15. Noise (pepper and salt) effect on ciphertext and recovery image in different degrees.



(**a**) Loss 50% (**b**) Loss 30% (**c**) Loss 20% (**d**) Loss 10%

(**e**) Recover loss 50% (**f**) Recover loss 30% (**g**) Recover loss 20% (**h**) Recover loss 10%

Figure 16. Data loss and recovery in different degrees.

4.11. Floating Frequency

According to Murillo-Escobar et al. [39] and Hosseinzadeh et al. [40], the floating frequency analysis serves as a crucial tool to assess the uniformity of the encryption process

employed on both the rows and columns of an image. It also evaluates the encryption's ability to generate uniformly distributed random data for all segments of the original image. By applying this robust analysis, any vulnerabilities or weak encryption areas within the cryptogram can be identified. The analysis is conducted by examining windows of 256 elements, arranged based on the image's rows and columns. The primary objective of the analysis is to quantify the number of differing elements within each window. In this study, we propose the concept of "rows' and columns' floating frequency" for a 256×256 gray-scale image. The methodology for calculating this floating frequency is as follows:

1. Select windows comprising 256 elements for each row and column of the image;
2. Count the number of distinct elements within each window, determining how many different elements are present;
3. Define the "row floating frequency" (RFF) and "column floating frequency" (CFF) as the frequencies of distinct elements within the corresponding windows;
4. Calculate the mean of both the RFF and CFF values; additionally, generate plots to visually represent the distributions of RFF and CFF across the image.

Figures 17 and 18 showcase the column and row floating frequency analysis results for both the Lena 256×256 plain image (P) and its corresponding encrypted image. The CFF values depict the frequencies of distinct elements within the columns of the images. This analysis offers valuable insights into the encryption process's impact on the distribution of elements in the image columns, highlighting any potential deviations from uniformity. A higher percentage of column floating frequency (CFF) in the encrypted image indicates the greater efficiency of the image encryption algorithm in generating a randomized cryptogram at the column scale. Similarly, a higher percentage of row floating frequency (RFF) in the encrypted image signifies the improved efficiency of the image encryption algorithm in producing a randomized cryptogram at the row scale.

4.12. Chosen/Known Plain Image Attack

According to Murillo-Escobar et al. [41], several image encryption algorithms, highly regarded for their remarkable statistical performance, have succumbed to vulnerabilities arising from the exploitation of chosen/known plain image attacks. In these attacks, different encryption keys can be employed to decrypt the cipher image of another encrypted image. The failure of the secret key used for the Pepper image to successfully decrypt the encrypted Lena image is illustrated in Figure 19.

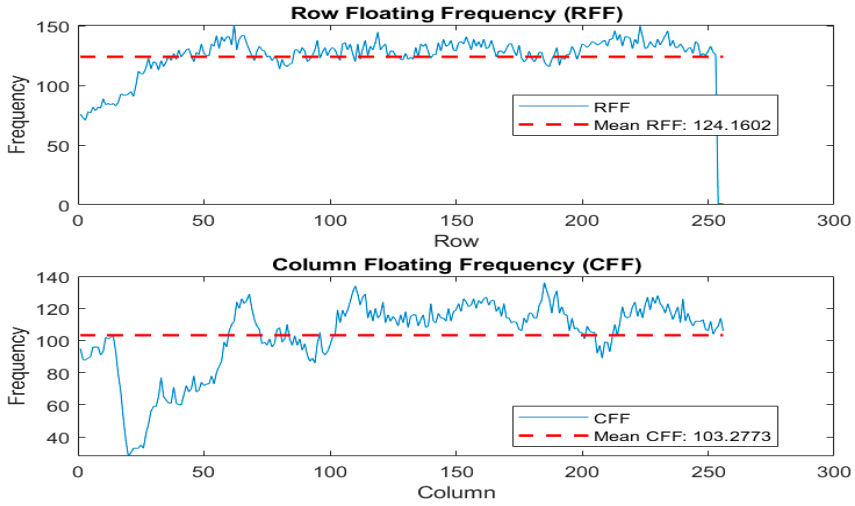


Figure 17. Row and column floating frequency and means for plain Lena image.

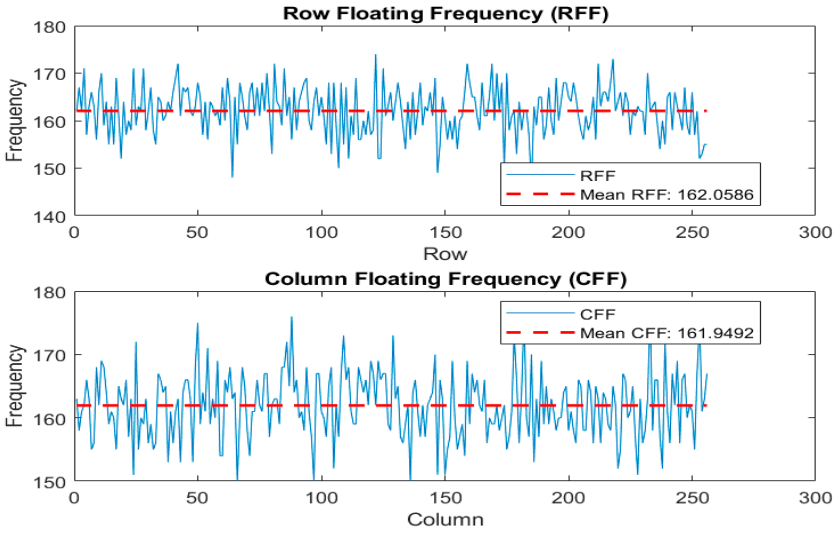
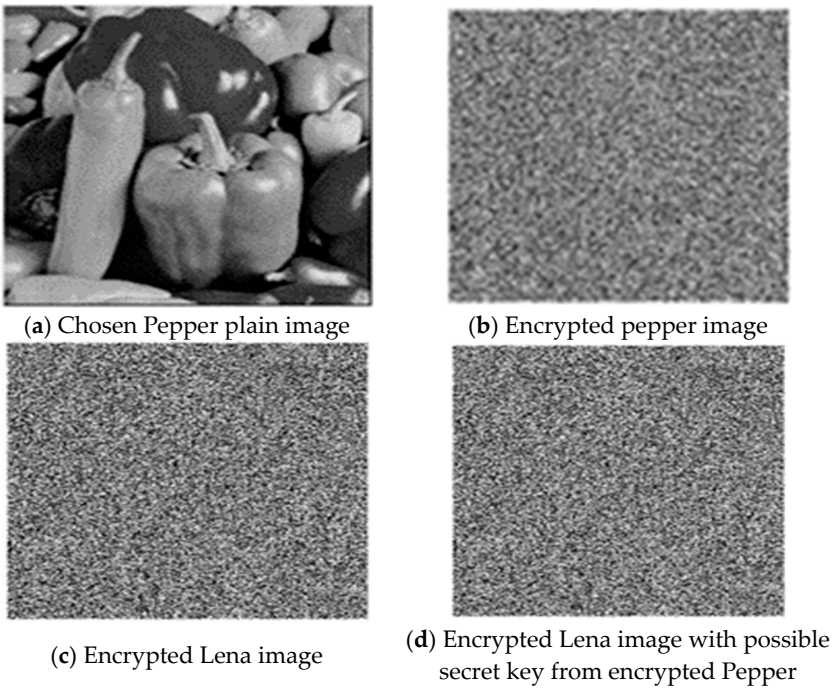


Figure 18. Row and column floating frequency and means for encrypted Lena image.



(**a**) Chosen Pepper plain image (**b**) Encrypted pepper image

(**c**) Encrypted Lena image (**d**) Encrypted Lena image with possible secret key from encrypted Pepper

Figure 19. Chosen/know plain image attack.

To enhance the proposed encryption scheme's resilience against cryptanalysis attacks, several measures have been implemented. In order to create a greater challenge for attackers who attempt brute-force attacks, the key size has been increased. K_1 and K_2 together have a total length of approximately $2^{65,536}$ key spaces, which makes them extremely robust against cryptanalysis attacks. Additionally, the scheme incorporates multiple rounds and utilizes various techniques, such as permutation, substitution, and diffusion, to enhance its robustness. Multiple chaotic maps have been incorporated into the key generation process, iteration numbers have been increased, and initial map conditions have been modified to make it even more complicated. Furthermore, the pixel scrambling process has been enhanced through the utilization of diverse techniques such as row–column scrambling and block-level scrambling. These collective measures contribute to fortifying the encryption scheme and bolstering its resistance against cryptanalysis attacks, ensuring heightened security for the encrypted data.

5. Conclusions

This paper presents a novel image encryption scheme that utilizes a hybrid chaotic map and fuzzy mathematics concept. The proposed approach employs a fuzzy triangular membership method to provide values that induce slight changes in all the initial condition parameters of the logistic sine map as well as the fuzzy Hénon map.

The utilization of the triangular membership function in generating the secret key allowed for the generation of additional secret keys by combining the triangular membership function with the Hénon map and the logistic sine map. The incorporation of the hybrid chaotic map design with triangular membership methods expands the potential secret key space, demonstrating a robust capability against sensitivity attacks after its use in image encryption.

While the proposed scheme in the paper does not directly fulfill the security requirements of non-repudiation and authentication, it effectively addresses the vital aspects of confidentiality, integrity, and availability. The system is intelligently designed to ensure continuous availability, even in the presence of faults such as noise data or data loss. Our techniques guarantee the encrypted image remains consistently accessible to legitimate entities. To uphold integrity, any modifications made to the encrypted text through this proposed scheme may produce different outcomes, primarily due to the sensitivity of the encryption keys. Maintaining confidentiality is a paramount concern as the information is meticulously safeguarded and accessible only to authorized parties.

The proposed scheme underwent various experiments, and the results were extensively analyzed and evaluated to verify its security capability. The testing and verification processes included statistical attack analysis, NIST tests, differential attack analysis, mean signal-to-noise ratio, signal-to-noise distortion ratio and mean error square, brute force attack analysis, and information entropy analysis. The mechanism demonstrated a high level of efficiency and met all the requirements necessary for the secure transmission of information by means of images.

Although the proposed scheme offers several advantages, there is still room for potential improvements in the future. The current design is limited to gray-scale images of size 256×256 and the use of triangular membership functions. It may be beneficial to explore other membership functions such as trapezoidal, Gaussian, quadratic, exponential, or even combinations of multiple methods to enhance the scheme's robustness. Another limitation of this study is that it may not be suitable for real-time applications due to its computational complexity. In upcoming research, we aim to address these limitations and further improve the encryption scheme.

Author Contributions: Conceptualization, D.E.M. and Y.X.; data curation, D.E.M., X.F., and X.W.; formal analysis, D.E.M. and X.F.; funding acquisition, X.F.; investigation, D.E.M. and X.W.; methodology, D.E.M.; project administration, X.W.; resources, D.E.M.; software, D.E.M.; supervision, X.F. and X.W.; validation, D.E.M. and X.W.; visualization, D.E.M. and X.F.; writing—original draft, D.E.M.; writing—review and editing, D.E.M. and Y.X. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the National Natural Science Foundation of China (No: 61672124), Password Theory Project of the 13th Five-Year Plan National cryptography Development Fund (no: MMJJ20170203), Liaoning Province science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105), and Jinan City 20 University Funding Projects Introducing Innovation Team Program (No: 2019GXRC03).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Available on request.

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. Du, W. *Computer Security: A Hands-on Approach*, 3rd ed.; Syracuse: New York, NY, USA, 2022.
2. Fu, C.; Lin, B.-B.; Miao, Y.-S.; Liu, X.; Chen, J.-J. A novel chaos-based bit-level permutation scheme for digital image encryption. *Opt. Commun.* **2011**, *284*, 5415–5423. [CrossRef]
3. Erkan, U.; Toktas, A.; Toktas, F.; Alenezi, F. 2D eπ-map for image encryption. *Inf. Sci.* **2022**, *589*, 770–789. [CrossRef]
4. Barker, E.; Mouha, N. *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. [CrossRef]
5. Dworkin, M.J. *Advanced Encryption Standard (AES)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. [CrossRef]
6. Rivest, R. *The MD5 Message-Digest Algorithm*; RFC 1321; Internet Engineering Task Force: Fremont, CA, USA, 1992. [CrossRef]
7. Pathak, B.; Pondkule, D.; Shaha, R.; Surve, A. Visual Cryptography and Image Processing Based Approach for Bank Security Applications. In *Second International Conference on Computer Networks and Communication Technologies*; Smys, S., Senjyu, T., Lafata, P., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 292–298. [CrossRef]
8. Teng, L.; Wang, X.; Xian, Y. Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. *Inf. Sci.* **2022**, *605*, 71–85. [CrossRef]
9. Wang, X.; Zhu, X.; Zhang, Y. An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map. *IEEE Access* **2018**, *6*, 23733–23746. [CrossRef]
10. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
11. Hua, Z.; Jin, F.; Xu, B.; Huang, H. 2D Logistic-Sine-coupling map for image encryption. *Signal Process.* **2018**, *149*, 148–161. [CrossRef]
12. Phatak, S.C.; Rao, S.S. Logistic map: A possible random-number generator. *Phys. Rev. E* **1995**, *51*, 3670–3678. [CrossRef]
13. Hénon, M. A two-dimensional mapping with a strange attractor. *Commun. Math. Phys.* **1976**, *50*, 69–77. [CrossRef]
14. Wang, X.-Q.; Zhang, H.; Sun, Y.-J.; Wang, X.-Y. A Plaintext-Related Image Encryption Algorithm Based on Compressive Sensing and a Novel Hyperchaotic System. *Int. J. Bifurc. Chaos* **2021**, *31*, 2150021. [CrossRef]
15. 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]
16. Mfungo, D.E.; Fu, X.; Wang, X.; Xian, Y. Enhancing Image Encryption with the Kronecker xor Product, the Hill Cipher, and the Sigmoid Logistic Map. *Appl. Sci.* **2023**, *13*, 4034. [CrossRef]
17. Valandar, M.Y.; Ayubi, P.; Barani, M.J. A new transform domain steganography based on modified logistic chaotic map for color images. *J. Inf. Secur. Appl.* **2017**, *34*, 142–151. [CrossRef]
18. Moysis, L.; Volos, C.; Jafari, S.; Munoz-Pacheco, J.M.; Kengne, J.; Rajagopal, K.; Stouboulos, I. Modification of the Logistic Map Using Fuzzy Numbers with Application to Pseudorandom Number Generation and Image Encryption. *Entropy* **2020**, *22*, 474. [CrossRef] [PubMed]
19. Rössler, O. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
20. Benedicks, M.; Carleson, L. The Dynamics of the Henon Map. *Ann. Math.* **1991**, *133*, 73. [CrossRef]
21. Sato, Y.; Doan, T.S.; Lamb, J.S.; Rasmussen, M. Rasmussen, Dynamical characterization of stochastic bifurcations in a random logistic map. *arXiv* **2018**, arXiv:1811.03994.
22. Bloch, I. Fuzzy spatial relationships for image processing and interpretation: A review. *Image Vis. Comput.* **2005**, *23*, 89–110. [CrossRef]
23. Ross, T.J. *Fuzzy Logic with Engineering Applications*, 3rd ed.; John Wiley & Sons: Hoboken, NJ, USA, 2010.
24. Zaman, J.K.; Ghosh, R. Review on fifteen Statistical Tests proposed by NIST. *J. Theor. Phys. Cryptogr.* **2012**, *1*, 18–31.
25. Nardo, L.G.; Nepomuceno, E.G.; Arias-Garcia, J.; Butusov, D.N. Image encryption using finite-precision error. *Chaos Solitons Fractals* **2019**, *123*, 69–78. [CrossRef]
26. Zhu, H.; Zhao, C.; Zhang, X.; Yang, L. An image encryption scheme using generalized Arnold map and affine cipher. *Optik* **2014**, *125*, 6672–6677. [CrossRef]
27. 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]
28. 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] [PubMed]
29. Wu, J.; Liao, X.; Yang, B. Image encryption using 2D Hénon-Sine map and DNA approach. *Signal Process.* **2018**, *153*, 11–23. [CrossRef]
30. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI Randomness Tests for Image Encryption. *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. (JSAT)* **2011**, *1*, 31–38.
31. 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]
32. Srivastava, R.; Singh, O. Performance Analysis of Image Encryption Using Block Based Technique. *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.* **2015**, *4*, 4266–4271.

33. Yavuz, E.; Yazıcı, R.; Kasapbaşı, M.C.; Yamaç, E. A chaos-based image encryption algorithm with simple logical functions. *Comput. Electr. Eng.* **2016**, *54*, 471–483. [CrossRef]
34. Carlson, A.; Gang, G.; Gang, T.; Ghosh, B.; Dutta, I.K. Dutta, Evaluating True Cryptographic Key Space Size. In Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), Online, 20 October 2021; IEEE: New York, NY, USA, 2021; pp. 243–249. [CrossRef]
35. Wu, Y.; Zhou, Y.; Saveriades, G.; Agaian, S.; Noonan, J.P.; Natarajan, P. Local Shannon entropy measure with statistical tests for image randomness. *Inf. Sci.* **2013**, *222*, 323–342. [CrossRef]
36. Yavuz, E. A new parallel processing architecture for accelerating image encryption based on chaos. *J. Inf. Secur. Appl.* **2021**, *63*, 103056. [CrossRef]
37. Wang, X.; Yang, J. A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient. *Inf. Sci.* **2021**, *569*, 217–240. [CrossRef]
38. Gao, X.; Mou, J.; Banerjee, S.; Cao, Y.; Xiong, L.; Chen, X. An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 1535–1551. [CrossRef]
39. Murillo-Escobar, M.A.; Meranza-Castillón, M.O.; López-Gutiérrez, R.M.; Cruz-Hernández, C. Suggested Integral Analysis for Chaos-Based Image Cryptosystems. *Entropy* **2019**, *21*, 815. [CrossRef] [PubMed]
40. Hosseinzadeh, R.; Zarebnia, M.; Parvaz, R. Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral. *Opt. Laser Technol.* **2019**, *120*, 105698. [CrossRef]
41. Murillo-Escobar, M.; Cruz-Hernández, C.; Abundiz-Pérez, F.; López-Gutiérrez, R.; Del Campo, O.A. A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal Process.* **2015**, *109*, 119–131. [CrossRef]