Hybrid Chaotic Based PRNG for Secure Cryptography Applications

Abdullah Alnajim , Ehab Abou-Bakr , Sarah Alruwisan , Sheroz Khan * , Rania Elmanfaloty *

Posted Date: 26 April 2023

doi: 10.20944/preprints202304.0974.v1

Keywords: Chaos; Encryption; SHA-256; NPCR; UACI

Article

Hybrid Chaotic Based PRNG for Secure Cryptography Applications

Abdullah M. Alnajim [1], Ehab Abou-Bakr [2,3], Sarah S. Alruwisan [4], Sheroz Khan [5,*] and Rania A. Elmanfaloty [6,7,*]

1 Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia; najim@qu.edu.sa
2 Department of Computer Science and Information Technology, Jeddah International College, 23831 Jeddah, Saudi Arabia; ehab.aboubakr@gmail.com
3 Department of Computer Engineering, The Higher Institute of Engineering and Technology, El-Behera, Egypt
4 Department of Architecture, College of Engineering and IT, Onaizah Colleges, Al-Qassim 56447, Saudi Arabia; sa14rahnet@gmail.com
5 Department of Electrical Engineering, College of Engineering and Information Technology, Onaizah Colleges, Onaizah 56447, PO Box 2053, Saudi Arabia; cnar32.sheroz@gmail.com
6 Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia
7 Department of Electronics and Communications Engineering, Alexandria Higher Institute of Engineering and Technology, Egypt; relmanfaloty@kau.edu.sa
* Correspondence: cnar32.sheroz@gmail.com; relmanfaloty@kau.edu.sa

Abstract: This paper suggests a novel one-dimensional (1D) map to address the limitations of traditional chaotic 1D maps. The main challenge with traditional chaotic 1D maps is the limited control parameter range and the potential risk of collapsing as a result under the finite precision implementation. To overcome these limitations, the new 1D map hybridises the traditional logistic map with tent map, and a linear tent-like function. This hybridization results in a wider range of control parameters to produce chaotic behavior. The dynamic behavior of the new 1D map has been analyzed using well known numerical methods, including the bifurcation diagram and Lyapunov exponent. Both tests have shown their complex and diverse behavior. In addition, a novel image encryption scheme has been devised using the new function as its pseudo-random-number generator. The proposed encryption algorithm has been tested and found to be robust and secure, passing all statistical tests applied to the encrypted images. The results of this study demonstrate the effectiveness of the new 1D map for use in secure image cryptography applications, providing a more robust and secure alternative to traditional chaotic 1D maps. The proposed algorithm has demonstrated high performance in NPCR and UACI tests. It also has shown good results in the MSE and PSNR tests.

Keywords: chaos; encryption; SHA-256; NPCR; UACI

1. Introduction

The need for privacy security has been felt intensely in the wake of so many multi-media and social platforms [1] generating significant amounts of unstructured data. To protect from unauthorized access and cyber-attacks sensitive information being transmitted through communication networks and the data that is being stored in cloud storage services, cryptographers have explored various methods of ciphering data. One method is obfuscation done to blur visual identity in photos and videos in order [2] to perturb or unsettle original data [3] for protecting personal information by encrypting the etymological origins of data [4], thus making data unreadable by unauthorized users. Another option is data masking [5], which involves obscuring parts of genomic data to make it unidentifiable during collection, which will make it staying unidentifiable during transmission and storage too.

 doi:10.20944/preprints202304.0974.v1

Tokenization [6] is another approach, which replaces sensitive data with non-sensitive data tokens that retain all essential elements of the data without risking its security to protect data confidentiality. Homomorphic encryption is a more complex method that allows computations to be performed on encrypted data without the need for decryption [7] that is primarily meant for non-cryptographers. The process of encryption is a commonly judged by the way how strong the proposed method stands for protection against different types of attacks [8,9]. It involves the use of an encryption mechanism using an encrypt key, a communication channel for data transmission, a decryption system, and a key to decrypt the encrypted data. The strength of an encryption system is determined by the attributes of the key, such as its secrecy, difficulty to guess, and ability to withstand against exhaustive search [10]. Each of these methods has its own benefits and limitations, and the appropriate method depends on the specific requirements and circumstances of each application [11,12]. The security of an encryption scheme is closely linked to the characteristics of the key the scheme uses. For an unbreakable scheme, the key should be truly random, better to be for use only once, and should be of the same length as the message, also called a one-time pad (OTP). However, these properties also have drawbacks. For instance, transmitting a key that is too long over a secure channel may not be practical, and it may make more sense to send the message itself through it. Furthermore, if the same key is utilized twice, the adversary may use XOR or frequency analysis to obtain information about the messages, and create a straightforward running key cipher in disguise.

Despite the importance of the strength of the key, other critically essential factors should be taken into account, including novel chaotic oscillator for the overall performance of an a novel design encryption system [13] covering potential perspectives of the proposed PRNG. The results are produced in the form of the cipher versions of images. These include the computational complexity of the mathematics representation, the size of generated key, and the unpredictable nature of the generated sequencing. In addition, the efficiency and practicality of an encryption algorithm should also be considered, as well as the availability of the necessary computational resources and the ease of key management, and particularly under the exceptional circumstances cases of COVID-19 [14], introducing Tokens Shuffling Approach (TSA) for better reliability during the pandemic.

Cryptologists have been tempted to use chaotic functions due to their simple mathematical representation and randomness [15] by applying the proposed algorithm to some original images to be reconstructed subsequently, achieving remarkable results in screening the colonoscopy images through neural networks (NN) [16]. The chaos-based image encryption techniques are highly efficient in case of multimedia data [17], using chaos game for encryption [18], making them ideal in terms of ease of implementation for cybersecurity applications [19]. While single 1D chaotic maps are low in cost for hardware implementation, they are inefficient in practice, as they have limited control parameters and can converge to a periodic orbit under finite precision implementation [20,21]. To address these issues, studies have proposed using 2D chaotic maps [22] that offer a balance between hardware complexity [23] and the chaotic performance [24].

This paper explores further the trend of expanding the number and range of control parameters of 1D maps [25] to achieve a wide ranging dynamic behavior [26] by introducing a new 1D map with embedded parameters for ensuring large scale better control of chaotic behavior. The paper is organised with Section 2 providing a literature overview of the well-known 1D maps, and Section 3 introducing the new 1D map and to present the results of verifying its chaotic behavior. In Section 4, a new image encryption algorithm is suggested that utilizes the map as pseudo-random number generator (PRNG). The robustness of the proposed encryption scheme is demonstrated by applying known attacks in Section 5 before concluding the paper in Section 6. The effectiveness of the proposed algorithm has been proven through rigorous testing, showing that it possess robustness with remarkable confusion-diffusion properties.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

2. Known 1D chaotic maps

2.1. Logistic map

Logistic maps make powerful tools for the examination of nonlinear systems, which have been applied to designing encryption schemes in various fields [27]. The simplicity of logistic map allows for a comprehensive understanding of the underlying dynamics [28], while its complexity can reveal random-like behavior [29]. It is represented by the discrete-time iterative equation (1) such that each iteration generates an iterate value:

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

Where $0 < x_n < 1$ is denoting the state of the system at the n^{th} iteration, and r is the control parameter that modulates the behavior of the system.

The behavior of the logistic map is contingent upon the value of the control parameter r. For $r < 1$, the logistic map converges to a fixed point of *zero*. As shown in Figure (1a) and (1d) where the various forms illustrate that for $1 < r < 4$ values, the map oscillates between fixed points in a bifurcation behavior. For $r = 4$ the solutions of the logistic map demonstrate chaos, implying that small variations in the initial conditions can result in fundamental differences in the long-term behavior of the system.

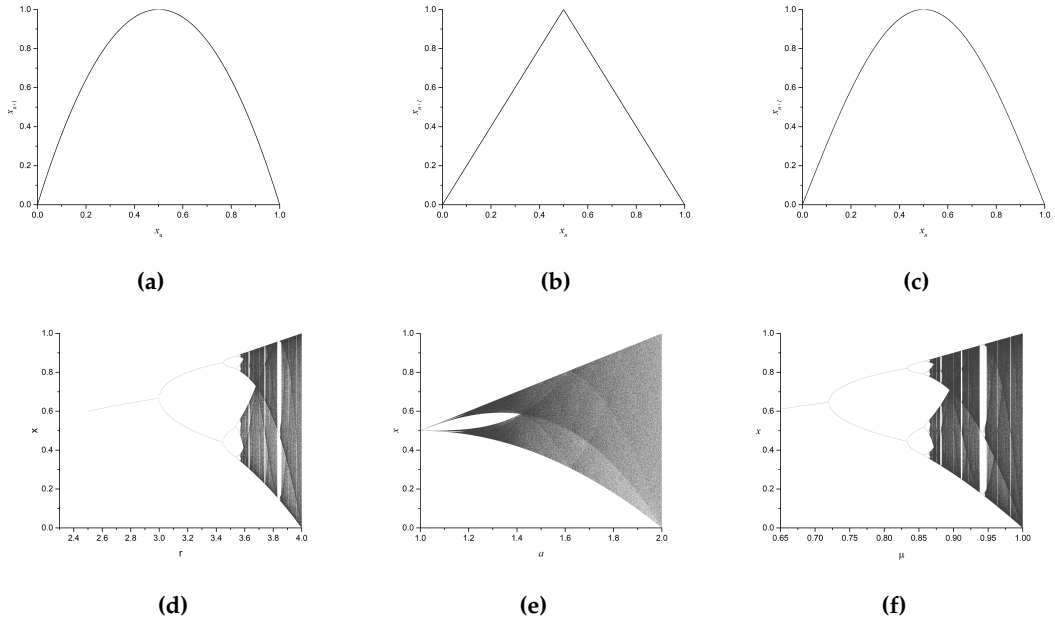


Figure 1. (**a**) Phase space of the logistic map, (**b**) Phase space of the tent map, (**c**) Phase space of the Sine map, (**d**) Bifurcation diagrams of the logistic map, (**e**) Bifurcation diagram of the tent map, (**f**) Bifurcation diagram of the Sine map.

2.2. Tent map

The tent map is a simple, discrete-time dynamical system that is often used to model chaos-based applications. It is defined by the piece-wise Equation (2):

$$x_{n+1} = \begin{cases} ax_n & \text{if } x_n < 0.5 \\ a(1 - x_n) & \text{if } x_n \geq 0.5 \end{cases} \tag{2}$$

Where x is the state variable, n is the time step, and a is the parameter. The range of the parameter a for $1 < a < 4$ between 0 and 2, determines the upper and lower limits of chaos in the system. For $a \leq 1$, the map is stable and periodic, while for $1 \leq a \leq 2$, the map is chaotic.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

The tent map is known for its tent-like characteristic shape of its graph, and it is one of the simplest examples of chaotic systems. It is often used as a prototypical first original example in the study of chaotic and nonlinear dynamics.

2.3. Sine map

The chaotic Sine map is a nonlinear function that exhibits complex and dynamic behavior. It is derived from the sine function defined in Equation (3):

$$x_{n+1} = \sin(\omega x_n) \tag{3}$$

Where ω is used as a control parameter that determines the behavior of the map Figure (1a). The chaotic Sine map has been widely explored for its potential applications in cryptography and image encryption due to its ability to generate apparently random and unpredictable sequences of numbers.

3. Modified 1D map

Although all the above mentioned maps are simple mathematical functions that have been individually used in the fields of cryptography alongside other domains. However, they have got certain limitations when it comes to generating pseudo-random sequences for use in the domain of cryptography. One of these limitations is the range of control parameters that results in a limited chaotic behavior. For example, in the case of the logistic map to be fully chaotic to fill the complete space range $f(x) : x \to x, x \in \Re : x \in [0, 1]$, the control parameter must be $r \approx 4$.

To overcome this limitation, a new function is introduced that consists of a combination of the logistic map as given in Equation (1), a piece-wise non-iterative linear tent map $y = 1 - |cx - 0.5c|$ of Equation (3), and finally the iterative tent map as given in Equation (2). The iterative 1D map is given by Equation (4):

$$x_{n+1} = \begin{cases} \frac{rx_n(1-x_n)(1-|cx-0.5c|+\mu x_n)}{2} & \text{if } x < 0.5 \\ \\ mod(rsin(\pi x_n)(1 - |cx - 0.5c| + \mu(1 - x_n)), 1) & \text{if } x \geq 0.5 \end{cases} \tag{4}$$

Where x_n and x_{n+1} show the present and next states respectively. The parameters r and μ are the control parameters for the logistic map and the tent map with approximate values of 4 and 2. The control parameter c is a global parameter that modifies the slope of the function and is used to create different dynamic behaviors as shown in Figure 2.

3.1. Sensitivity to control parameters and initial condition

The sensitivity of this system to small changes in the initial conditions or the control parameter c is a key aspect to consider when studying its dynamics. Small changes in the initial conditions can lead to vastly different behavior in the long term, resulting in a highly sensitive system. Similarly, small changes in the value of the control parameter c can lead to significant changes in the system dynamics. This is clearly depicted in Figure 3 where perturbations of 10^{-6} in any of the initial conditions or control parameters have produced two completely different sequences.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

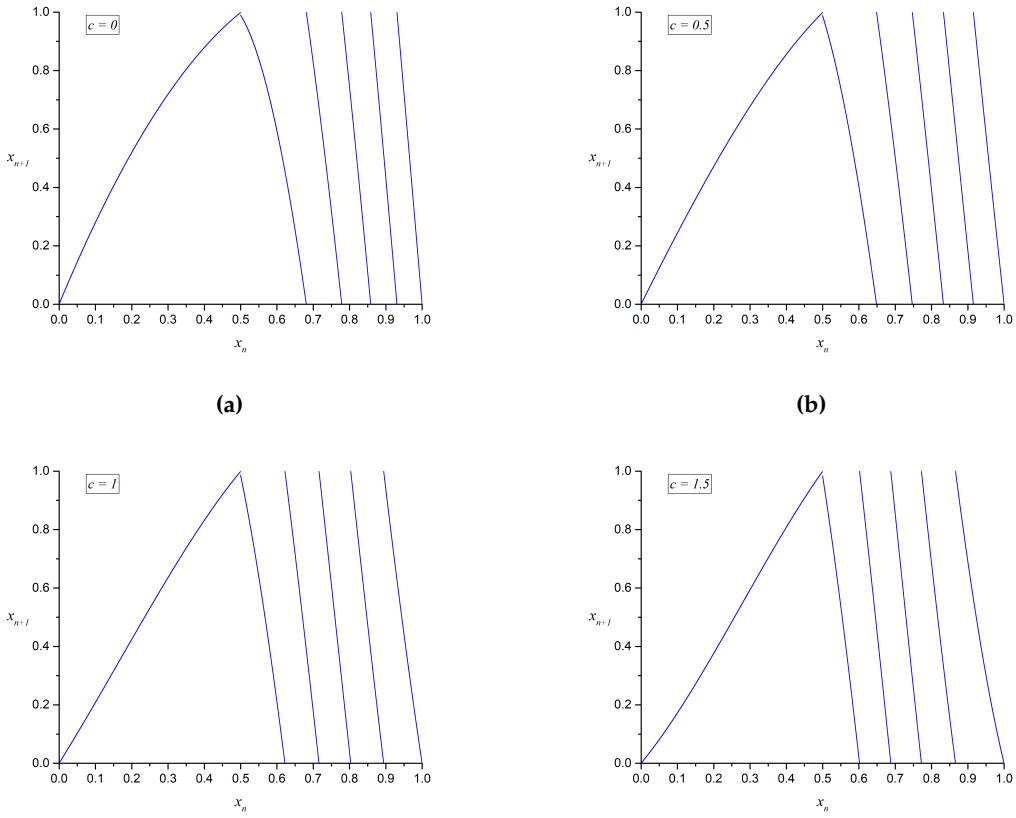


Figure 2. Phase space for the map described in Equation (4), (**a**) for $c = 0$, (**b**) for $c = 0.5$, (**c**) for $c = 1$, and (**d**) for $c = 1.5$.

This property is crucial for ensuring the security and robustness of encryption systems that rely on chaotic-nature of the resulting PRNGs. Even a small variations in the initial state can lead to vastly different output sequences, making it extremely difficult for an attacker to predict or reproduce the sequence without having knowledge of the initial conditions.

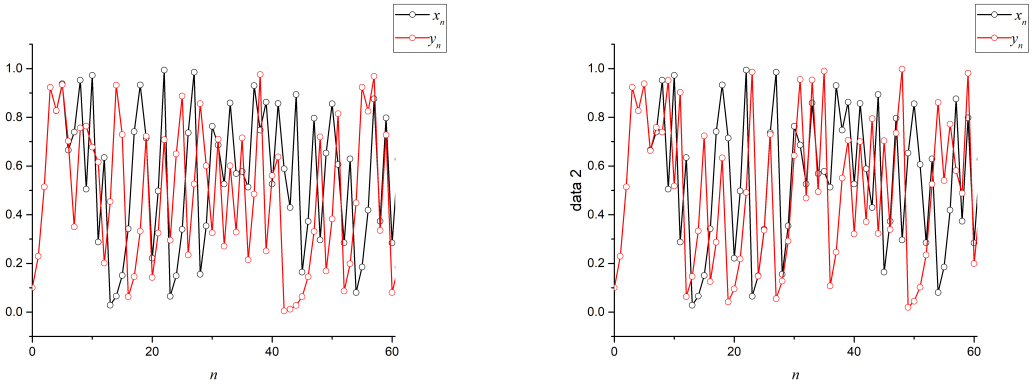


Figure 3. Sensitivity to small perturbations for iterates of the map described in Equation (4) for two state variables x & y , (a) when $x_o = 0.01$ & $y_o = x_o + 10^{-6}$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

3.2. Bifurcation diagram

The bifurcation diagram of the function of Equation (4) is a powerful tool for understanding its dynamic behavior. Figure 4 shows visual representation of how the system changes in its response to changes in the control parameter c. The function does not exhibit any of the usual dynamic behavior consisting of a sequence in the regions of stable fixed points, periodic orbits and then chaos. Instead, when setting $r = 4$ and $\mu \approx 2$ while varying c, the function shows full chaotic behavior over the range of $0 \leq c \leq 2$.

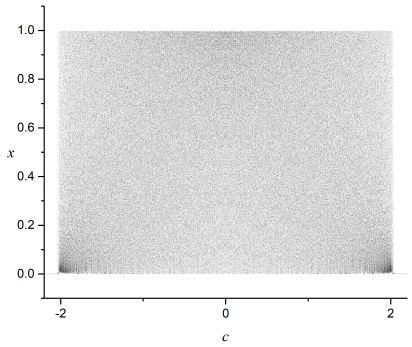
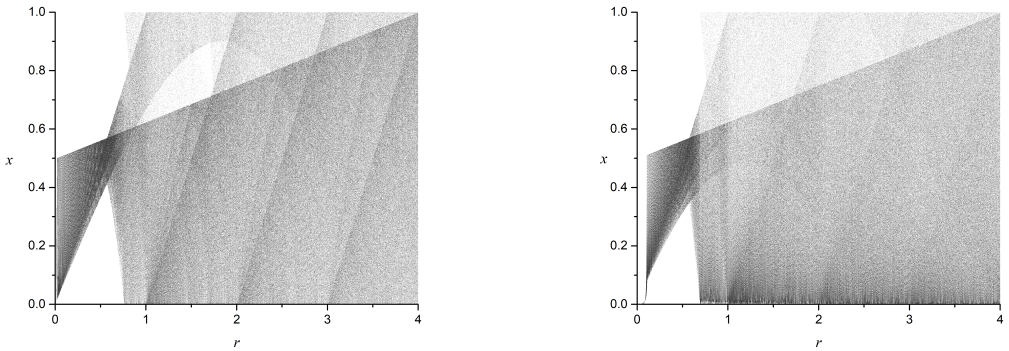


Figure 4. Bifurcation diagram of the function given by Equation (4) showing full chaotic behavior in the range of $0 \leq c \leq |2|$.

It is also worth noting that the function can also show chaotic behavior for a range of r values and specific values of c as can be seen in Figure 4. This suggests that the system behavior is not solely determined by the control parameter c, but also by other parametric values of r. However, in this manuscript, we have chosen to focus on studying the properties of the function for changes only the control parameter c. This allows for a more in-depth analysis of the system's behavior that relates to this specific parameter.



(a) **(b)**

Figure 5. Examples of the bifurcation diagram of (4) depending on r when (a) $c = 0.1$, (b) $c = 1.8$

3.3. Lyapunov exponent

The Lyapunov Exponent (LE) is a mathematical tool used to measure the rate of separation of nearby trajectories in a dynamic system. It is an important concept in the study of chaos theory and provides a measure of the sensitivity of the system's behavior to initial conditions.

The Lyapunov Exponent is calculated by taking the average rate of change of the distance between two nearby trajectories over time. It is represented mathematically as given in Equation (5):

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \frac{|\delta_1|}{|\delta_o|} \tag{5}$$

Where, λ denotes the LE, while δ_1 and δ_o show the spacing between the two trajectories. The positive Lyapunov Exponent implies that the system is sensitive to initial conditions and that small variations in initial conditions will grow exponentially over time, leading to vastly varying outcomes. To calculate the Lyapunov Exponent numerically, one can use the method in [30]. which involves linearizing the system of equations at a given point and then iterating the linearized equations to calculate the exponential growth rate of the distance between nearby trajectories.

Figure 6 shows that function of Equation (4) has a $\lambda > 0$ in the range of $-2 \leq c \leq 2$. This indicates that the system is chaotic within this range of the control parameter c, as the Lyapunov Exponent measures the rate of separation of the nearby trajectories, and a positive exponent implies exponential divergence.

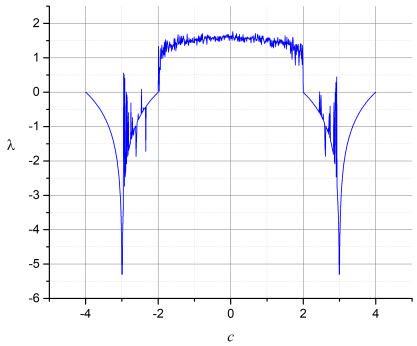


Figure 6. Lyapunov exponent of the function in (4) showing positive values in the range of $-2 \leq c \leq 0$.

4. Proposed Encryption Algorithm

Image encryption is a critical component of the information security domain, particularly in the domain of digital communication. With the proliferation of images being exchanged over various networks, the need for robust and secure image encryption algorithms has become increasingly important. The goal of image encryption is to convert an image into a ciphertext, which is unreadable to anyone unless it is decrypted. The encrypted image should remain confidential, even if intercepted by any cybernetic attacker.

The image encryption process must be secure, providing a high level of protection against various attacks, including brute force attacks and statistical attacks. In addition, the encryption process must be efficient and capable of performing real-time applications. The importance of image encryption cannot be underemphasized, especially in the case of sensitive images, such as medical or military images, which require the highest level of protection.

In this paper, the image encryption method is described in detail, providing a technical and mathematical analysis of the encryption process. The focus is on developing an efficient and secure image encryption algorithm that satisfies the requirements expected for protection of such levels. The algorithm will be tested and evaluated using various statistical tests producing results discussed in detail.

4.1. Encryption steps

The proposed image encryption algorithm is based on a permutation-confusion process that utilizes the proposed chaotic function as its core Pseudo-Random Number Generator (PRNG) with different keys k_1 and k_2.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

The overall key K is composed of two sub-keys, k_1 and k_2, each of which has a length of 128 bits, with the least significant 64 bits representing the parameter x_0 and the most significant 64 bits representing the parameter c. The generation of these keys is performed through the following steps:

Step 1: Key generation

The 256-bit sequence, referred to as the hash, is generated using the Sha256 algorithm. Key k_1 uses the least 128 bits and k_2 uses the most 128 bits. The values of x_0 and c for each key are derived from the hash using Equation (6) to Equation (9):

$$x_{0,k_1} = \frac{\sum_{i=0}^{63} 2^i \cdot hash(i+1)}{2^{64}} \tag{6}$$

$$c_{k_1} = \frac{2 \cdot \sum_{i=0}^{63} 2^i \cdot hash(i+65)}{2^{64}} \tag{7}$$

$$x_{0,k_2} = \frac{\sum_{i=0}^{63} 2^i \cdot hash(i+129)}{2^{64}} \tag{8}$$

$$c_{k_2} = \frac{2 \cdot \sum_{i=0}^{63} 2^i \cdot hash(i+193)}{2^{64}} \tag{9}$$

These equations ensure that x_0 and c stay in the ranges $0 \leq x_0 \leq 1$ and $0 \leq c \leq 2$.

Step 2: Permutation stage:

In the permutation stage, a simple and effective algorithm is used to break the correlation between adjacent pixels in the message image, which is an important step for securing the scheme against statistical attacks. This is achieved by using the dimension of the original image $[M \times N]$ and the subkey k_1 to generate a sequence using the function $f(k_1)$. The permuted pixels are then sorted based on this generated sequence.

The permutation process starts by reading a grayscale message image (I_m) with size $[M \times N]$. Each pixel in the image is converted to its binary form (B). The image is then reshaped into a 1D array. The sequence is generated from a Pseudorandom Number Generator (PRNG) using Equation (4) with a length of $W \times n$, where $n = M \times N$ and $W \in \{3, 4, 5, 6\}$. The subsequence of length n is extracted from this generated sequence. This subsequence is sorted while keeping the sorted element original index. The pixels in 1D I_m are also sorted based on this generated sequence.

Step 3: Confusion stage:

In the confusion stage, the goal is to increase the resistance against differential attacks by ensuring that any small change in the original image leads to nonuniform spreading across the ciphered image.

To achieve this, a stream y_i is generated from the function $f(k_2)$ and used to replace the bit level value of each encrypted pixel using the equation (10):

$$C_i = I_{m_i} \oplus floor(mod(y_i \; times 10^4, 256)) \tag{10}$$

Where I_m is the permuted pixels, y is the generated sub-sequence, and C_i is the resulting image after the confusion step.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

5. Results and Analysis

The algorithm is considered to be secure if it can effectively defend against any known forms of attacks including brute-force key attack, statistical attacks, and similar types of known attacks. The proposed method is evaluated using various security analysis techniques to demonstrate its robustness. The analysis has been carried out using a 64-bit double-precision floating point representation, implemented using 64-bit MATLAB (R2020a) on a Windows 11 operating system, running on a Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz machine with 16 GB of RAM.

5.1. Encryption quality analysis

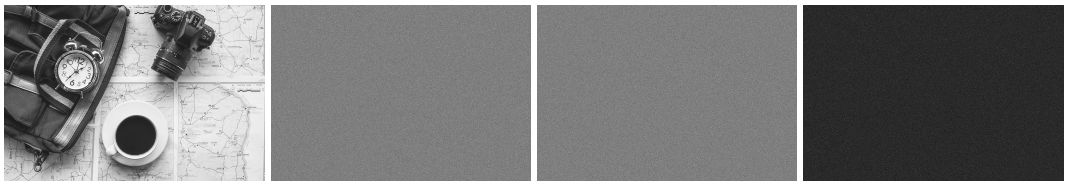
5.1.1. Key space analysis

The proposed encryption algorithm utilizes two keys, k_1 and k_2, in its permutation and confusion stages, respectively. Both keys consist of a control parameter c and an initial condition x_0. The key space of the algorithm is determined by the range of possible values for c and x_0. It is safe to say that even with the fastest computers available today the time required to brute-force a 256-bit key would be much greater than than the estimated age of the universe. For example, consider a 64-bit key, a typical Intel(R) Core(TM) i7 computer with a clock speed of 1.8 billion cycles per second would take approximately 5.8×10^{16} years to perform a brute-force attack on a 64-bit key. This demonstrates the importance of selecting strong cryptography keys in order to ensure the security and integrity of sensitive information.

Further, both keys are designed to have a large key-space in the floating point representation format, which ensures that the encryption algorithm is secure against key brute-force attacks. The use of different keys for the permutation and confusion stages further increases the security of the encryption algorithm by making it more difficult for an attacker to crack the encryption open for a grasp of the message.

5.1.2. Key sensitivity analysis

The results of encryption algorithm's sensitivity to changes analysis are presented in Figure 7, where a pixel-by-pixel subtraction has been performed between two encrypted images, $\nabla I' = |I'_1(K_1) - I'_2(K_2)|$, using two slightly different keys K_1 and K_2, where K_1 and K_2 differ only by a small amount in one of their control parameters such that $\delta = K_1(c_1) - K_2(c_2) < 10^{-8}$.
The noisy appearance of encrypting a high resolution image 3264×4841 I' in Figure (7d) confirms that the algorithm produces different encrypted images, I'_1 using K_1 in Figure (7b) and I'_2 using K_2 in Figure (7d).



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

Figure 7. Sensitivity of the encryption algorithm to small change in the key K. (**a**) original high resolution image 3264×4841 , (**b**) encrypted image I'_1 obtained using K_1, (**c**) encrypted image I'_2 obtained using $K_2 = K_1 + 10^{-8}$ in one ot its control parameters c, and (**d**) the absolute pixel-by-pixel difference between I'_1 and I'_2, which confirms the production of two distinct encrypted images.

5.1.3. MSE and PSNR

The Mean Squared Error (MSE) measures the average of the squared differences between the original and the encrypted image. The lower MSE value indicates that the encrypted image is more similar to the original image, and so a lower MSE value image has a lower level of distortion.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

The Peak Signal-to-Noise Ratio (PSNR) is a measure of the quality of the encrypted image compared to the original image. It is calculated as the ratio of the maximum possible power of a signal and the power of the distortion caused by the encryption process. The higher PSNR value indicates that the encrypted image is of higher quality and has less distortion compared to the original image as a result of encryption.

To further demonstrate the robustness of the proposed method, the previously mentioned tests have been conducted by making slight changes to keys k_1 and k_2. The Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) have been calculated using Equation (11) and Equation (12):

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{i,j} - q_{i,j})^2 \tag{11}$$

$$PSNR = 20log_{10}\frac{(MAX_p)}{\sqrt{MSE}} \tag{12}$$

Where m and n are the number of rows and columns in the image, p is the original image and q is the embedded image. The results of these calculations are listed in Table 1, showing two encrypted images c_1 and c_1 as a function of variations in the keys k_1 and k_2. The obtained numbers confirm the sensitivity of the scheme to small changes in the key. Since k_1 is used for permuting the pixels and k_2 is used for changing the gray levels, the results in the table demonstrate that the scheme has shown a good level of confusion-diffusion properties.

Table 1. Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) of two encrypted images.

Changed Parameter	MSE	PSNR(dB)
k_1	10.872×10^3	7.767
k_2	10.921×10^3	7.748

Table 1 shows the MSE and PSNR values of two encrypted images that were generated by changing the parameters k_1 and k_2 in an image encryption scheme. Both MSE values are relatively high, indicating that the ciphered images are significantly different from the original image. Meanwhile, both PSNR values are relatively low, indicating that the level of distortion in the ciphered images is high compared to the original image.

This is a desirable property of a good image encryption scheme since it implies that the ciphered image has undergone both confusion and diffusion.

5.1.4. Histogram Analysis

The distribution of color intensities in an image can be visualized through a histogram. The more robust encryption scheme should result in an encrypted image with a more uniform histogram, even if the original image had a weak intensity distribution. The histograms of the original images have unique intensity distributions that characteristically representing the images as shown in Figure 8. In contrast, the histograms of all the encrypted images exhibit a uniform shape, showing no unique features for potential decryption purposes. This indicates that the proposed algorithm can effectively resist statistical attacks.

5.1.5. Correlation Analysis

The security of an image against statistical attacks is often dependent on the correlation between adjacent pixels. A robust encryption scheme should aim to break this correlation in the (V) vertical, (H) horizontal, and (D) diagonal directions. To quantify this, we calculate the correlation coefficient between pairs of adjacent pixels, denoted by r_{xy}. This is done by selecting S random pairs of adjacent pixels and substituting them into the Equation (13) to Equation (18):

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

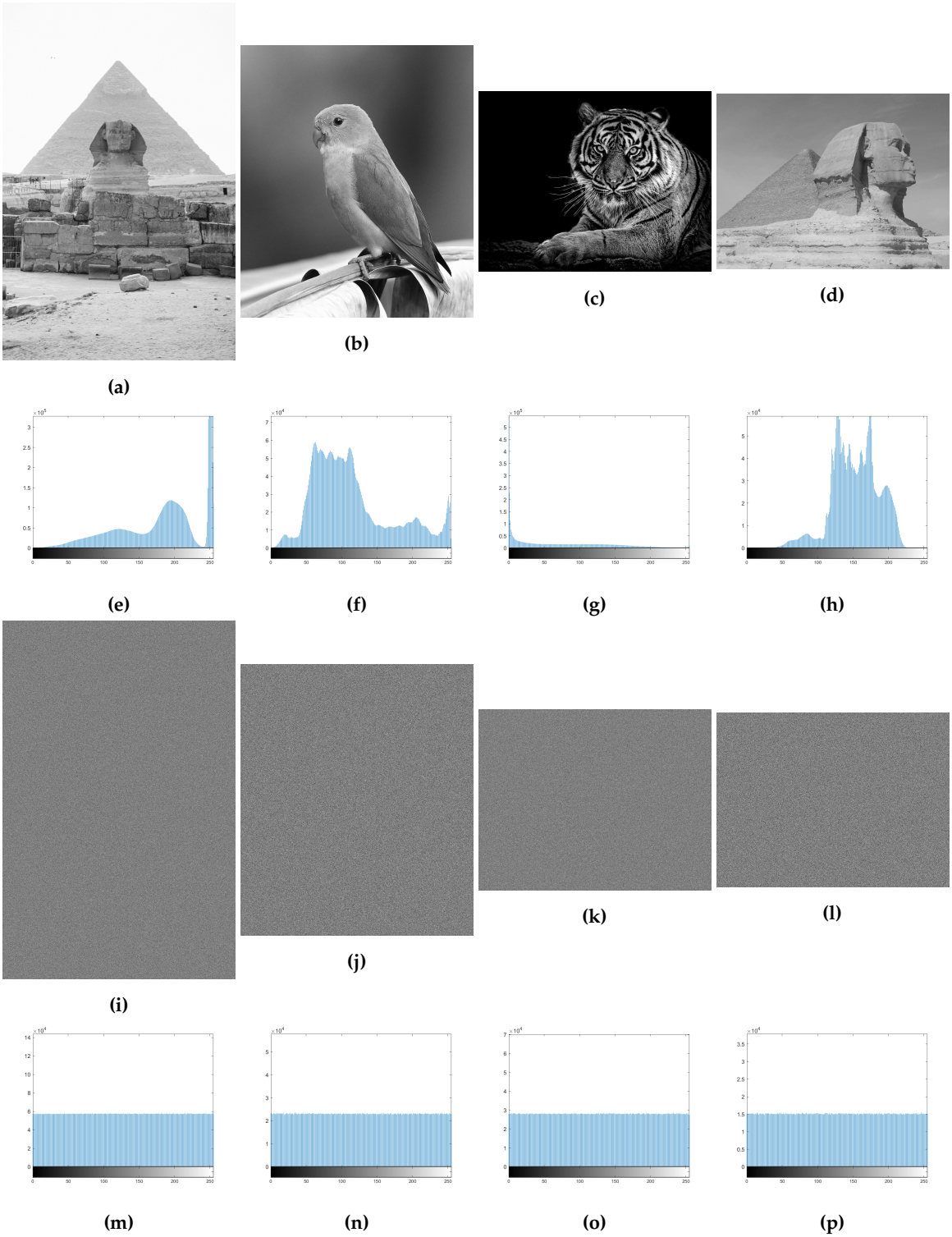


Figure 8. Comparison of encrypted images with original images, their histograms, encrypted versions, and histograms of encrypted images (displayed vertically) is shown, with each subfigure labeled as: (**a**–**d**) original image, (**e**–**h**) histogram, (**i**–**l**) encrypted image, (**m**–**p**) histogram of encrypted image.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

$$D(x) = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))^2 \tag{13}$$

$$D(y) = \frac{1}{S}\sum_{i=1}^{S}(y_i - E(y))^2 \tag{14}$$

$$E(x) = \frac{1}{S}\sum_{i=1}^{S}x_i \tag{15}$$

$$E(y) = \frac{1}{S}\sum_{i=1}^{S}y_i \tag{16}$$

$$cov(x,y) = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))(y_i - E(y)) \tag{17}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{18}$$

Where x_i and y_i are the values of the selected adjacent pixels. The results of this calculation are as shown in Figure 9, which demonstrate that the correlation is strong and compact in the original image, but scattered and weak in the encrypted image. Further results of this analysis for different images are as listed in Table 4, which show that all of the encrypted images have weak correlation and hence show resilience against statistical attacks.

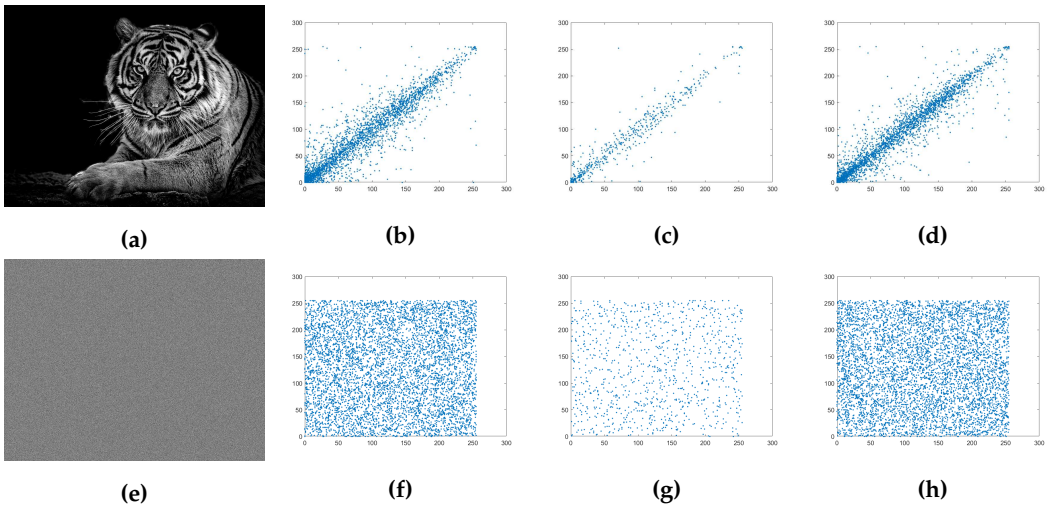


Figure 9. Correlation analysis of 3000 of adjacent pixels in an original and encrypted image include: (**a**) the original image, (**b**) its diagonal correlation, (**c**) its horizontal correlation, (**d**) its vertical correlation, (**e**) the encrypted image, (**f**) its diagonal correlation, (**g**) its horizontal correlation, and (**h**) its vertical correlation.

Table 2. Vertical, horizontal and diagonal correlation of some images and their encrypted ones.

		Original image			*Ciphered image*		
File name	*Size*	*V-correlation*	*H-correlation*	*D-correlation*	*V-correlation*	*H-correlation*	*D-correlation*
bird.png	2625x2250	0.9876	0.9736	0.9706	-6.46E-04	0.0188	-0.0061
lion.png	2362x3047	0.971	0.9764	0.957	0.0189	-0.0164	0.0198
pyramids.png	4755x3090	0.9894	0.9908	0.9841	-0.0033	-0.038	0.0143
sphinx.png	1704x2272	0.9793	0.9839	0.9733	0.0253	0.0126	0.0058

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

5.1.6. Information Entropy

The benefit of using entropy as a measure of information security in cryptography is that it provides a quantitative measure of the uncertainty or randomness in the data distribution, which is directly related to the security of the ciphering algorithm. The higher entropy value indicates a more uniform distribution of data and less information to be extracted from it, resulting in a more secure ciphering algorithm. Entropy is a measure of the overall randomness of an image or a system that is as expressed by Equation (19):

$$H = -\sum_{i=1}^{2^n} P(m_i) \log_2 P(m_i) \tag{19}$$

Where n represents the number of bits of the color intensity, and $P(m_i)$ is the probability of a color intensity, m_i, in the image. The higher the entropy value the more uniform distribution will be the encrypted image leaving almost nothing as information that can be extracted from the image. Local Shannon entropy, on the other hand, analyzes the randomness of the image at a local scale. The local entropy of non-overlapping blocks of an image is calculated using Equation (20):

$$LSE = \frac{1}{k} \sum_{i=1}^{k} H(I_{B_i}) \tag{20}$$

Where k is the number of blocks, $H(I_{B_i})$ is the Shannon entropy of the block. In this paper, the significant values are $\alpha = 0.05$, $\alpha = 0.01$, $\alpha = 0.001$, k = 30 and block size of 1936 pixels. In cryptography, the higher the entropy of an encrypted image, the more secure it is considered to be, as it contains less information that can be extracted by an attacker. Table 3 shows to confirm that the proposed scheme falls within this critical interval of different image sizes.

Table 3. Global and local Shannon entropy of the proposed algorithm.

File name	Size	Global entropy		Local Shannon entropy		
				$\alpha = 0.05$	$\alpha = 0.01$	$\alpha = 0.001$
				$h^{l*}_{left} = 7.901901305$	$h^{l*}_{left} = 7.901722822$	$h^{l*}_{left} = 7.901515698$
		original Image	Encrypted Image	$h^{l*}_{right} = 7.903037329$	$h^{l*}_{right} = 7.903215812$	$h^{l*}_{right} = 7.903422936$
bird	2625×2250	7.559383165	7.999966812	7.902673265	7.902100541	7.902336555
lion	2362×3047	4.868976964	7.999975018	7.902084826	7.902600108	7.902215068
pyramids	4755×3090	6.840163701	7.999988669	7.902317244	7.90294224	7.902561135
sphinx	1704×2272	6.951101185	7.999956064	7.902838446	7.901851957	7.902802677

5.2. Resistance to differential attack

Net Pixel Change Rate (NPCR)

NPCR is a measure of the robustness of an image encryption algorithm. It is defined as the percentage of pixels in a given encrypted image that change when one bit of the original image changes. NPCR is commonly used to evaluate the strength of an encryption algorithm against chosen-plaintext attacks, where an attacker attempts to determine the encryption key by observing how changes to the plaintext affect the encrypted image. The NPCR is given by Equation (21) and Equation (22):

$$NPCR = \frac{\sum_{i=1}^{N} [C_i \neq E_i]}{N} \times 100 \tag{21}$$

$$\mathcal{N}^*_\alpha = \frac{L + \Phi^{-1}(\alpha)\sqrt{L/T}}{L+1} \tag{22}$$

Where N is the total number of pixels in the encrypted image, C_i and E_i are the i-th pixel values of the original image and the encrypted image, respectively. The numerator of the equation counts the number of pixels that differ between the original and encrypted images, and the denominator

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 April 2023 doi:10.20944/preprints202304.0974.v1

normalizes this count to the total number of pixels in the image. The resulting percentage value gives a measure of the NPCR of the encryption algorithm. The higher the NPCR value, the more robust will be the algorithm against chosen plain-text attacks.

Table 4. NPCR and UACI score results for 26 images with different sizes.

		NPCR test result				*UACI test result*		
File name	*Score%*	*Status*	Ref.[26]	Ref.[25]	*Score %*	*Status*	Ref.[26]	Ref.[25]
Dimention 256×256		$\mathcal{N}_\alpha^* \geq 99.5527\%$			$\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+} = (33.2255\%, 33.7016\%)$			
5.1.09	99.6094	pass	99.588	99.5941	33.4659	pass	33.5688	33.4722
5.1.10	99.5773	pass	99.6689	99.5728	33.4735	pass	33.5222	33.6179
5.1.11	99.585	pass	99.5743	99.5743	33.5218	pass	33.4894	33.5225
5.1.12	99.5789	pass	99.6277	99.5758	33.3434	pass	33.4975	33.3374
5.1.13	99.617	pass	99.5712	99.6459	33.5078	pass	33.5465	33.5497
5.1.14	99.5895	pass	99.5697	99.6170	33.2638	pass	33.5711	33.5752
Dimention 512×512		$\mathcal{N}_\alpha^* \geq 99.581\%$			$\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+} = (33.3445\%, 33.5826\%)$			
5.2.08	99.5956	pass	99.5998	99.5918	33.429	pass	33.5446	33.4202
5.2.09	99.5895	pass	99.6086	99.6040	33.4564	pass	33.4976	33.3967
5.2.10	99.6014	pass	99.6048	99.5987	33.411	pass	33.3785	33.5028
7.1.01	99.6052	pass	99.5934	99.6014	33.4872	pass	33.4887	33.4886
7.1.02	99.6193	pass	99.6094	99.6056	33.5014	pass	33.5073	33.4162
7.1.03	99.612	pass	99.6025	99.5975	33.4781	pass	33.4612	33.5348
7.1.04	99.6136	pass	99.6189	99.6006	33.4653	pass	33.5243	33.4449
7.1.05	99.6357	pass	99.6094	99.6109	33.3931	pass	33.4804	33.4587
7.1.06	99.6033	pass	99.6105	99.6113	33.4627	pass	33.4292	33.4813
7.1.07	99.6086	pass	99.6078	99.5968	33.3644	pass	33.4592	33.4569
7.1.08	99.6147	pass	99.6052	99.6117	33.4791	pass	33.4667	33.4746
7.1.09	99.6204	pass	99.604	99.6151	33.5324	pass	33.4781	33.4900
boat.512	99.6067	pass	99.6365	99.6009	33.4882	pass	33.4683	33.3759
gray21.512	99.5876	pass	99.6178	99.5937	33.4121	pass	33.545	33.4828
ruler.512	99.6239	pass	99.6231	99.6021	33.4651	pass	33.4407	33.4163
Dimention 1024×1024		$\mathcal{N}_\alpha^* \geq 99.5952\%$			$\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+} = (33.4040\%, 33.5231\%)$			
5.3.01	99.6078	pass	99.6063	99.6078	33.4627	pass	33.4725	33.4706
5.3.02	99.6084	pass	99.602	99.6009	33.483	pass	33.4983	33.4801
7.2.01	99.5984	pass	99.6073	99.6010	33.4672	pass	33.4723	33.4664
Dimention 1704×1704		$\mathcal{N}_\alpha^* \geq 99.602\%$			$\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+} = (33.4326\%, 33.4945\%)$			
sphinx	99.6099	pass	-	-	33.4517	pass	-	-
Dimention 2362×2362		$\mathcal{N}_\alpha^* \geq 99.604\%$			$\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+} = (33.4408\%, 33.4863\%)$			
lion	99.6079	pass	-	-	33.4658	pass	-	-
Dimention 2625×2625		$\mathcal{N}_\alpha^* \geq 99.6034\%$			$\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+} = (33.4385\%, 33.4886\%)$			
bird	99.6108	pass	-	-	33.4701	pass	-	-
Dimention 4755×4755		$\mathcal{N}_\alpha^* \geq 99.6056\%$			$\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+} = (33.4476\%, 33.4794\%)$			
pyramids	99.6081	pass	-	-	33.4597	pass	-	-

Unified Average Changing Intensity (UACI)

UACI is a metric used to calculate the difference in average intensity between two encrypted images, denoted as C and C'. The difference is calculated using equation (23):

$$UACI(C, C') = \sum_{i,j} \frac{|C(i,j) - C(i,j)|}{T \times L} \tag{23}$$

Where L is the maximum level of color intensity and T is the total number of pixels in the image. The result of UACI is declared as "Pass" if it falls within the interval $[\mathcal{U}_\alpha^{*-}, \mathcal{U}_\alpha^{*+}]$.

Where $\mu_\mathcal{U}$ and $\sigma_\mathcal{U}$ are given by Equation (25) and Equation (26):

$$\mu_\mathcal{U} = \frac{L+2}{3L+3} \tag{24}$$

$$\sigma_\mathcal{U} = \frac{(L+2)(L^2+2L+3)}{18(L+1)^2LT} \tag{25}$$

In this article, 27 grayscale images of different sizes and intensities are subjected to both the NPCR and UACI tests with $\alpha = 0.05$. The results in Table 4 show that all scores are with PASS grades, indicating that the proposed system has good confusion and diffusion properties that make them to withstand differential attacks while ensuring data security.

6. Discussion and Conclusion

This paper has introduced a novel 1D chaotic function that exhibits complete chaotic behavior across a broad range of a single control parameter $c \in [-2, 2]$. This new chaotic function has been utilized as the core of a Pseudo-Random Number Generator (PRNG) in an image encryption proposed scheme, which has been subjected to various tests to determine its robustness. The key space analysis has indicated that the proposed scheme had a key space size of 256 bits, which is sufficient to withstand brute force attacks. The sensitivity analysis has demonstrated that the scheme has been sensitive to any small changes in the key, with acceptable values of Mean Squared Error (MSE) Peak Signal-to-Noise Ratio (PSNR). The histogram analysis has revealed a uniform distribution of pixel values, indicating good image quality after encryption. The algorithm also passed the entropy analysis test for significant parameter values of $\alpha = \{0.05, 0.01, 0.01\}$, indicating high randomness in the generated PRNs. Moreover, the proposed encryption scheme has been found to be resistant to differential attacks based on the results of testing it on 28 grayscale images of various sizes for NPCR and UACI. Overall, the tests have demonstrated that the proposed image encryption scheme, which employs a hybrid chaotic map as its PRNG, exhibits good confusion and diffusion properties. These findings contribute to the field of image encryption and chaos-based cryptography by providing a suitable solution for systems that possess a wide range of chaotic behavior in their control parameters. The proposed scheme can be utilized for secure transmission and storage of confidential images.

Author Contributions: Conceptualization, Rania A. Elmanfaloty and Ehab Abou-Bakr; methodology, Abdullah M. Alnajim; software, Sarah S. Alruwisan; validation, Rania A. Elmanfaloty and Ehab Abou-Bakr; formal analysis, Abdullah M. Alnajim; investigation Sheroz Khan; resources, Sheroz Khan; data curation, Rania A. Elmanfaloty and Ehab Abou-Bakr; writing—original draft preparation, Abdullah M. Alnajim, Ehab Abou-Bakr; writing—review and editing, Sarah S. Alruwisan, Sheroz Khan; visualization, Sarah S. Alruwisan; supervision, Rania A. Elmanfaloty; project administration, Abdullah M. Alnajim; funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Wang, C.; Tianqing, Z.; Xiong, P.; Ren, W.; Choo, K.K.R. A privacy preservation method for multiple-source unstructured data in online social networks. *Computers & Security* **113**, 102,574 (2022).
2. Sun, Q.; Tewari, A.; Xu, W.; Fritz, M.; Theobalt, C.; Schiele, B. In Proceedings of the European conference on computer vision (ECCV) (2018); pp. 553-569.
3. Cunha, M.; Mendes, R.; Vilela, J.P. A survey of privacy-preserving mechanisms for heterogeneous data types. *Computer science review* **41**, 100,403 (2021).
4. Zhao, Y.; Chen, J. A survey on differential privacy for unstructured data content. *ACM Computing Surveys (CSUR)* **54**, *10s*, 1–28 (2022).
5. Ghadirli, H.M.; Nodehi, A.; Enayatifar, R. An overview of encryption algorithms in color images. *Signal Processing* **164**, 163–185 (2019).
6. Gagliardelli, L.; Zecchini, L.; Ferretti, L.; Beneventano, D.; Simonini, G.; Bergamaschi, S.; Orsini, M.; Magnotta, L.; Mescoli, E.; Livaldi, A. et al. A big data platform exploiting auditable tokenization to promote good practices inside local energy communities. *Future Generation Computer Systems* **141**, 595–610 (2023).
7. Fontaine, C.; Galand, F. A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security* **2007**, 1–10 (2007).
8. Taleby Ahvanooey, M.; Li, Q.; Hou, J.; Rajput, A.R.; Chen, Y. Modern text hiding, text steganalysis, and applications: a comparative analysis. *Entropy* **21**, *4*, 355 (2019).

9. Thakkar, B.; Thankachan, B. A Survey for Comparative Analysis of various Cryptographic Algorithms used to Secure Data on Cloud. *Int. J. Eng. Res. Technol* **9**, *08*, 753–756 (2020).
10. Cao, C.; Tang, Y.; Huang, D.; Gan, W.; Zhang, C. IIBE: an improved identity-based encryption algorithm for WSN security. *Security and Communication Networks* **2021**, 1–8 (2021).
11. Yazdeen, A.A.; Zeebaree, S.R.; Sadeeq, M.M.; Kak, S.F.; Ahmed, O.M.; Zebari, R.R. FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. *Qubahan Academic Journal* **1**, *2*, 8–16 (2021).
12. You, X.; Wang, C.X.; Huang, J.; Gao, X.; Zhang, Z.; Wang, M.; Huang, Y.; Zhang, C.; Jiang, Y.; Wang, J. et al. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. *Science China Information Sciences* **64**, 1–74 (2021).
13. El-Latif, A.A.A.; Ramadoss, J.; Abd-El-Atty, B.; Khalifa, H.S.; Nazarimehr, F. A Novel Chaos-Based Cryptography Algorithm and Its Performance Analysis. *Mathematics* **10**, *14*, 2434 (2022).
14. Bahbouh, N.; Basahel, A.; Sendra, S.; Sen, A.; Ahmed, A. Tokens Shuffling Approach for Privacy, Security, and Reliability in IoHT under a Pandemic. *Applied Sciences* **13**, *1*, 114 (2023).
15. Pourasad, Y.; Ranjbarzadeh, R.; Mardani, A. A new algorithm for digital image encryption based on chaos theory. *Entropy* **23**, *3*, 341 (2021).
16. Zhang, W.; Fu, C.; Zheng, Y.; Zhang, F.; Zhao, Y.; Sham, C.W. HSNet: A hybrid semantic network for polyp segmentation. *Computers in Biology and Medicine* **150**, 106,173 (2022).
17. Kumar, S.; Srivastava, P.K.; Srivastava, G.K.; Singhal, P.; Singh, D.; Goyal, D. Chaos based image encryption security in cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography* **25**, *4*, 1041–1051 (2022).
18. Pour, N.R.; Yaghoobi, M. A new method in encryption of gray scale images using chaos game representation. *Multimedia Tools and Applications* **81**, *20*, 29,653–29,672 (2022).
19. Salleh, M.; Ibrahim, S.; Isnin, I.F. In Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03., vol. 2 (IEEE, 2003), pp. II–II.
20. Elmanfaloty, R.A.; Abou-Bakr, E. Random property enhancement of a 1D chaotic PRNG with finite precision implementation. *Chaos, Solitons & Fractals* **118**, 134–144 (2019).
21. AbdElHaleem, S.H.; Abd-El-Hafiz, S.K.; Radwan, A.G. A generalized framework for elliptic curves based PRNG and its utilization in image encryption. *Scientific Reports* **12**, *1*, 13,278 (2022).
22. Boriga, R.E.; Dăscălescu, A.C.; Diaconu, A.V. A new fast image encryption scheme based on 2D chaotic maps. *IAENG International Journal of Computer Science* **41**, *4*, 249–258 (2014).
23. Akhshani, A.; Behnia, S.; Akhavan, A.; Hassan, H.A.; Hassan, Z. A novel scheme for image encryption based on 2D piecewise chaotic maps. *Optics Communications* **283**, *17*, 3259–3266 (2010).
24. Zhu, L.; Jiang, D.; Ni, J.; Wang, X.; Rong, X.; Ahmad, M.; Chen, Y. A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. *Signal Processing* **195**, 108,489 (2022).
25. Elmanfaloty, R.A.; Abou-Bakr, E. An image encryption scheme using a 1D chaotic double section skew tent map. *Complexity* **2020**, 1–18 (2020).
26. Elmanfaloty, R.A.; Alnajim, A.M.; Abou-Bakr, E. A finite precision implementation of an image encryption scheme based on DNA encoding and binarized chaotic cores. *IEEE Access* **9**, 136,905–136,916 (2021).
27. Khairullah, M.K.; Alkahtani, A.A.; Bin Baharuddin, M.Z.; Al-Jubari, A.M. Designing 1D chaotic maps for fast chaotic image encryption. *Electronics* **10**, *17*, 2116 (2021).
28. Moysis, L.; Tutueva, A.; Volos, C.; Butusov, D.; Munoz-Pacheco, J.M.; Nistazakis, H. A two-parameter modified logistic map and its application to random bit generation. *Symmetry* **12**, *5*, 829 (2020).
29. 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* **22**, *4*, 474 (2020).
30. Sprott, J.C. *Chaos and time-series analysis*, vol. 69; Oxford university press: New York, 2003.