Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.040858
Article

A Novel Parallel Computing Confidentiality Scheme Based on Hindmarsh-Rose Model

Jawad Ahmad[1,*], Mimonah Al Qathrady[2], Mohammed S. Alshehri[3], Yazeed Yasin Ghadi[4], Mujeeb Ur Rehman[5] and Syed Aziz Shah[6]

[1]School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, EH10 5DT, UK
[2]Department of Information Systems, College of Computer Science and Information Systems, Najran University, Najran, 61441, Saudi Arabia
[3]Department of Computer Science, College of Computer Science and Information Systems, Najran University, Najran, 61441, Saudi Arabia
[4]Department of Computer Science, Al Ain University, Abu Dhabi, 112612, United Arab Emirates
[5]School of Science, Technology and Health, York St John University, York, YO31 7EX, UK
[6]Research Centre for Intelligent Healthcare, Coventry University, Coventry, CV1 5FB, UK
*Corresponding Author: Jawad Ahmad. Email: J.Ahmad@napier.ac.uk
Received: 01 April 2023; Accepted: 29 May 2023; Published: 30 August 2023

Abstract: Due to the inherent insecure nature of the Internet, it is crucial to ensure the secure transmission of image data over this network. Additionally, given the limitations of computers, it becomes even more important to employ efficient and fast image encryption techniques. While 1D chaotic maps offer a practical approach to real-time image encryption, their limited flexibility and increased vulnerability restrict their practical application. In this research, we have utilized a 3D Hindmarsh-Rose model to construct a secure cryptosystem. The randomness of the chaotic map is assessed through standard analysis. The proposed system enhances security by incorporating an increased number of system parameters and a wide range of chaotic parameters, as well as ensuring a uniform distribution of chaotic signals across the entire value space. Additionally, a fast image encryption technique utilizing the new chaotic system is proposed. The novelty of the approach is confirmed through time complexity analysis. To further strengthen the resistance against cryptanalysis attacks and differential attacks, the SHA-256 algorithm is employed for secure key generation. Experimental results through a number of parameters demonstrate the strong cryptographic performance of the proposed image encryption approach, highlighting its exceptional suitability for secure communication. Moreover, the security of the proposed scheme has been compared with state-of-the-art image encryption schemes, and all comparison metrics indicate the superior performance of the proposed scheme.

Keywords: Hindmarsh-rose model; image encryption; SHA-256; parallel computing

1 Introduction

Chaos is a ubiquitous phenomenon in nature, and nonlinear science heavily relies on the study of chaos. Chaos theory, with its fundamental characteristics such as system unpredictability, parameter sensitivity, pseudo-randomness, and others, has found applications in various precise disciplines. In recent years, the practical advantages of chaos theory have gained significant attention. Chaos theory has numerous practical uses, including in the secure transmission of multimedia data. Specifically, when data is exchanged over the Internet. Images of national defense and private information are just two examples of a few private images that must be communicated securely [1–3]. When it comes to protecting sensitive data, encryption is crucial. The two most common older methods for encrypting data are the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). The high correlation among neighbouring pixels in digital images is one distinguishing feature; the relative insensitivity to change is another; minor adjustments to pixel values do not lead to noticeably different images from those already in the database [4–6]. Hence, standard encryption approaches are unsuitable for image data encryption due to their time complexity etc. A plethora of image security solutions has been proposed in the literature [7–9] to address the aforementioned issue. High-speed encryption, complexity, strong security, and a manageable computer resource overhead are all features of chaos-based secure communication. For real-world use cases, it can be adopted for image and text encryption.

Ye et al. [10] proposed that diffusion and confusion are the two main building blocks of image encryption. Diffusion refers to the connection between the unencrypted text and the encrypted representation of it. The efficacy of an encryption method increases if even a small shift in the initial image falls out into a noticeable shift in the enciphered image. In this context, "confusion" refers to the connection between the hidden key and the ciphertext representation. When making slight changes to the encryption key, resulting in noticeably different encrypted images, it is generally accepted that the encryption is highly secure.

1.1 Literature Review

The role that chaos plays in cryptography is also influenced by its characteristics. Mutually continuous-time and discrete-time chaotic maps can be distinguished from the mathematical model description of chaotic systems. There are many common models of continuous-time chaotic systems, but two of the most common are the Lorenz system and the Chen system. Arnold maps, logistic maps, sine maps, and Henon maps are examples of models for discrete chaotic systems. Another methodology for categorizing chaotic systems distinguishes between systems with integer forms and systems with fractional forms. The model of a fractional system is more general. Hénon-Lozi type maps [11], for example, are examples of recently proposed typical fractional chaotic maps that display a rich complicated dynamic behaviour. After proposing a hyperchaotic fractional Grassi-Miller map in [12], the authors proceed to implement it in hardware. A chaotic map with fractional order is presented and investigated in [13]. Several books and articles discuss the utilization of chaos for image encryption.

A fast and secure image encryption system was proposed by Khennaoui et al. [14], and it makes use of a 1D chaotic map. The composition of a 1D chaotic system is straightforward, even though the key space is very small. When it comes to protecting images, 1D chaotic maps provide advantages such as increased speed and simpler hardware implementation. Chaotic encryption research excels in the field of image encryption due to the synergy between effective chaotic systems and challenging encryption approaches. In [9], a sine trigonometric function and tent map are utilized to propose a discrete chaotic system. The statistical behaviour is consistent over a large range of parameter

values. Piecewise linear chaotic mapping and a trigonometric function were used by Liu et al. [15] to create the chaotic mapping. Li et al. [16] discussed a nonlinear dynamic system that includes a cosine function and finds that it has a lengthy chaotic interval and resilient chaotic qualities. The inverse of a trigonometric function is likewise a trigonometric function because trigonometric functions have unique qualities such as periodicity and boundedness. A 1D piecewise chaotic map and the bisection approach were presented for image encryption in [17]. Elghandour et al. [18] employed a hyperchaotic model to produce a pseudo-random sequence, which they subsequently encrypted using a combination of scrambling and diffusion. Gopalakrishnan et al. [19] generated a new 1D chaotic model using the Beta function and applied it to image encryption; they called their proposal the Beta chaotic map. Zahmoul et al. [20] proposed an innovative image cryptosystem that employs a hybrid chaotic system by combining two 1D chaotic maps. The pseudo-orbits of one-dimensional chaotic systems are employed as the key in an innovative encryption method presented by Alawida et al. [21]. Nepomuceno et al. [22] designed and implemented a one-dimensional sine-powered chaotic map for image encryption. As part of an effective symmetric image encryption scheme, Mansouri et al. [23] proposed a novel 2D chaotic map to expand the available key space. Using a 2D economic chaotic map and a logistic map, Huang et al. [24] devised a method for encrypting images. Askar et al. [25] propose an innovative method of encryption that uses keys generated from either DNA or an image of plaintext. Khan et al. [26] introduced an S-Box and logistic-sine scheme for image encryption.

The research discussed above has led to the proposal of secure cryptosystems. However, it is worth noting that many of these proposals may suffer from either insecurity or impracticality issues, primarily related to time complexity. Therefore, considering the time cost as a crucial factor, we focused on improving the efficiency of the system. To achieve better security, we employed a simple chaotic map available, which exhibits high randomness.

1.2 Research Contribution

Many encryption algorithms do not offer strong security against classical cryptographic attacks [27–29]. The cryptanalysis of many recently proposed cryptosystems has increased the risk of sensitive information being lost. Therefore, by considering all the weaknesses carefully, we have constructed a secure encryption algorithm to provide image security. We have proposed a multiplication and diffusion-based encryption strategy based on the Hindmarsh-Rose chaotic model [1]. The key generation process is secured by the SHA-256 hashing algorithm. The proposed technique employs an image's associated encryption key as a substitute for the traditional encryption key, which increases security and reduces the amount of time it takes to decrypt data [30,31]. The encryption method combines a scrambling process with a diffusion process.

1.3 Paper Organization

The subsequent sections of this manuscript are organised as follows: Section 2 offers a comprehensive analysis of the Hindmarsh-Rose model; Section 3 discusses the construction of the proposed model. In the next two sections, we have shown simulation outcomes and performance analysis, respectively. Finally, the conclusion with some future recommendations is presented in the last section.

2 Hindmarsh-Rose Model

The Hindmarsh-Rose model is a mathematical representation of the spiking-bursting behaviour detected in research with single neurons [1]. It focuses on the membrane potential, represented by the dimensionless variable $x(t)$, as well as the transportation of particles all through ion channels, which is measured by two additional variables: $y\,(t)$ and z(t). Specifically, $y\,(t)$ represents the ratio of sodium and potassium ion transport through fast ion channels, while $z\,(t)$ corresponds to an adaptation current that decreases the firing rate by incrementing at every spike. The Hindmarsh-Rose model entails a structure of three nonlinear ordinary differential equations that explain the behaviour of $x\,(t)$, $y\,(t)$, and $z\,(t)$. The Hindmarsh-Rose system is a three-variable dynamical model given by the subsequent set of equations:

$$\begin{cases} \dfrac{dx}{dt} = y - ax^3 + bx^2 - z + I_{ext}, \\ \dfrac{dy}{dt} = c - dx^2 - y, \\ \dfrac{dz}{dt} = r\,(s\,(x - x_0) - z), \end{cases} \tag{1}$$

where x, y, and z represent the state variables of the system, I_{ext} is the external current input, and a, b, c, d, r, s, and x_0 are the model parameters.

2.1 Stability Analysis

To find the equilibrium points, we set the derivatives in the above equations to zero and solve for x, y, and z:

$$\begin{cases} \dfrac{dx}{dt} = 0 \Rightarrow y - ax^3 + bx^2 - z + I_{ext} = 0, \\ \dfrac{dy}{dt} = 0 \Rightarrow c - dx^2 - y = 0, \\ \dfrac{dz}{dt} = 0 \Rightarrow r\,(s\,(x - x_0) - z) = 0, \end{cases} \tag{2}$$

where x is the membrane potential, y and z are the gating variables for the two potassium currents, a, b, c, d, r, s, and x_0 are model parameters, and I is an external current input.

We will use the following parameter values for the stability analysis: $a = 1.0$, $b = 3.0$, $c = 1.0$, $d = 5.0$, $r = 0.001$, $s = 4.0$, $x_0 = -1.6$, $I = 4.0$.

To determine the fixed points of the model, we solve the equations $\dfrac{dx}{dt} = \dfrac{dy}{dt} = \dfrac{dz}{dt} = 0$ simultaneously. This gives us the following three fixed points:

$$\begin{cases} (x_1, y_1, z_1) = (-1.7756, -3.5858, -5.4656), \\ (x_2, y_2, z_3) = (-1.5347, -0.0068, -0.0036), \\ (x_3, y_3, z_3) = (1.6703, -1.2098, 5.1926). \end{cases} \tag{3}$$

To examine the stability of the fixed points, compute the Jacobian matrix J evaluated at each fixed point. The Jacobian matrix is given by:

$$J = \begin{bmatrix} -3ax^2 + 2bx & 1 & -1 \\ -2dx & -1 & 0 \\ rs & 0 & -r \end{bmatrix}, \tag{4}$$

where x, y, and z are the values of the fixed point. We evaluate J at every fixed point and calculate the eigenvalues. The eigenvalues of J for each fixed point are:

Fixed point 1: $(-10.8647, -0.0378 + 0.2021i)$

The real part of all eigenvalues is negative, so the fixed point is stable.

Fixed point 2: $(1.6439, -1.1188 + 0.2491i)$

One eigenvalue has a positive real part, so the fixed point is unstable.

Fixed point 3: $(-6.2145, -1.9401 + 0.0000i)$

The real part of both eigenvalues is negative, so the fixed point is stable.

Therefore, we have one unstable fixed point and two stable fixed points. This means that the system can exhibit different types of behaviour depending on the initial conditions. If the initial conditions are near the unstable fixed point, the system will diverge and exhibit chaotic behaviour. If the initial conditions are instead near a stable fixed point, the system will converge towards that point and exhibit stable behaviour. The behaviour of a dynamical system is largely determined by its fixed points, which are values of the system's variables that do not change over time. Stable fixed points act as attractors, pulling the system towards them, while unstable fixed points act as repellers, pushing the system away from them.

2.2 Simulation of Hindmarsh–Rose Neuron

To examine the execution of the Hindmarsh-Rose model we have performed simulations based on different times. The spiking-bursting behaviour findings are explained in Fig. 1.

2.3 NIST Randomness Analysis

The National Institute of Standards and Technology (NIST) developed a widely used suite of tests for measuring the random behaviour of time series. Each sequence being evaluated is 1,000,000 bits in length, hence testing many sequences is necessary. Random performance of time series may be measured with the help of the p-value. The standard deviation is set to $= 0.01$. We produced 500 chaotic real number categorizations, individually with a length of 125,000 real numbers, to assess the stochastic recital of sequences produced using the chaotic map. For the NIST evaluation, one hundred sequences of length one million bits are obtained. Table 1 summarizes our experimental findings and comparative results with the existing chaotic map. Each p-value is bigger than 0.01, and the run test has a minimum pass rate of 96%, as can be seen from the test outcome. All chaotic sequences created by system (1) have been shown to pass the NIST test in experiments.

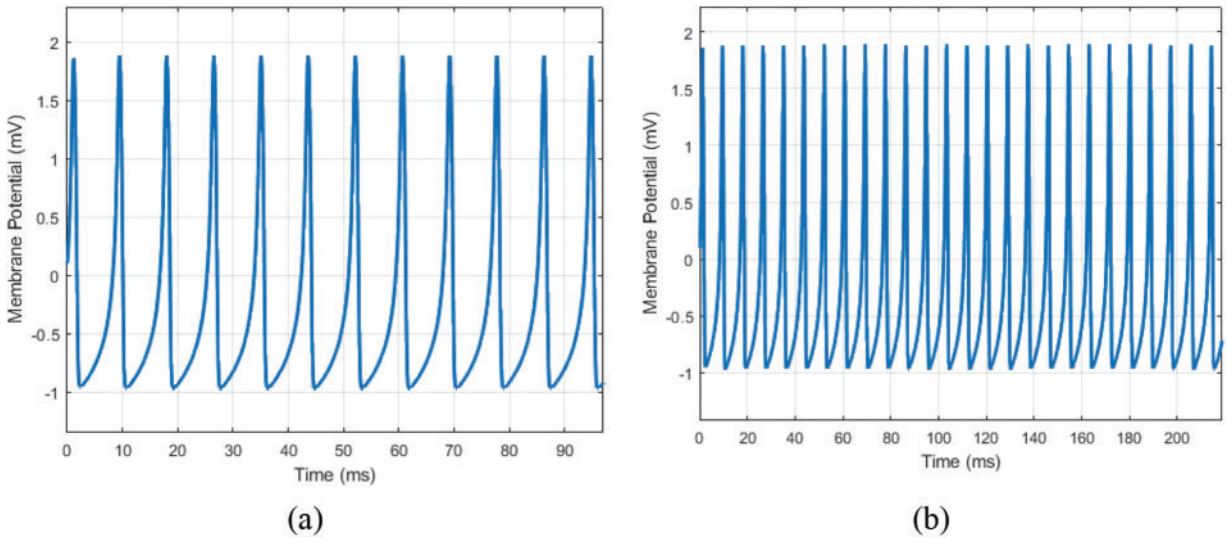

Figure 1: Hindmarsh-Rose neuron model for (a) 100-time span; (b) 220-time span

Table 1: NIST test outcome for Hindmarsh–Rose model

Test	*p*-value		Status
	Proposed	Ref. [32]	
Frequency	0.9194	0.024356	✓
Block frequency	0.9457	0.043087	✓
Runs	0.2919	0.856359	✓
Longest runs	0.0537	0.836048	✓
Universal	0.9099	0.366918	✓
Linear complexity	0.5427	0.408275	✓
Discrete fourier transform (Spectral)	0.8961	0.254411	✓
Overlapping template matching	0.9904	0.088762	✓
Non-overlapping template matching	0.8710	0.515882	✓
Approximate entropy	0.9813	0.936823	✓
Serial	0.9756	0.599693	✓
Cumulative sums	0.7908	0.429923	✓
Binary matrix rank	0.9125	0.530120	✓
Random excursions	0.9989	0.522378	✓
Random excursions variant	0.9167	0.47474	✓

3 Proposed Cryptosystem

In this section, we have proposed a novel image encryption scheme. The security of the encryption entirely varies on the input of the encryption algorithm. The proposed encryption approach comprises

two sub-algorithms named key generation and encryption/decryption processes defined in detail below:

3.1 Private Key Generation

The initial conditions and the key parameters of the proposed encryption algorithm are generated by inserting the input image in the SHA-256 algorithm. The results generated from SHA-256 are utilized as key parameters of the Hindmarsh-rose chaotic model. The first step was using the SHA-2 256 hash method to get the encryption key from the hash of the plaintext picture. The initial state value of the chaotic Hindmarsh-Rose system was determined by dividing the hash string into four parts, each of which was then mapped to a decimal larger than 0 and less than 1.

3.2 Encryption/Decryption Process

In this study, the colour digital image is encrypted by combining the operation of diffusion and invertible matrix multiplication generated from the Hindmarsh chaotic map. The notion of secure key generation from SHA-256 makes the encryption secure against statistical attacks. The major operations involved in the cryptosystem are matrix multiplication and diffusion. The array for diffusion is generated from the Hindmarsh-Rose model. The arrays constructed for the matrices are filtered through the inverse operation to make the decryption possible. The steps of the proposed encryption are as follows:

Step 1: The size of the input image is $m \times n \times 3$ in the encryption.

Step 2: The layers of the plain image are separated into red, green, and blue channels.

Step 3: Each layer is divided into blocks of 2×2 matrices.

Step 4: The invertible matrices generated from the Hindmarsh-rose model are then multiplied with the plain image matrices, respectively.

Step 5: The multiplicated results are then diffused with the key arrays generated from the Hindmarsh-Rose model.

Step 6: The resultants are then concatenated as cipher images.

The decryption of the ciphertext is performed in the same step in a reverse manner. The detailed working strides of the decryption process are as follows:

Step 1: The cipher image of size $m \times n \times 3$ is inserted as the input of the decryption algorithm.

Step 2: Inverse diffusion is applied to the layer of the cipher image.

Step 3: The resultant from Step 2 is then multiplied with the inverse of the private key constructed from the Hindmarsh-Rose model.

Step 4: The outcome layers from Step 3 are then combined into one plain image.

The working mechanism of the proposed encryption work is shown in Fig. 2.

4 The Simulation Results

To examine the implementation of the proposed cryptosystem, we have applied the encryption process over some standard colour images. The images of Baboon, Parrots, Peppers, and Tulip with sizes $512 \times 512 \times 3$ are selected to execute the encryption algorithm. The plain images and their respective encipher results are displayed in Fig. 3. The visual analysis of the encipher images exhibits

that the ciphered data do not expose any pattern about the primary image, which indicates the excellent quality of the encryption.

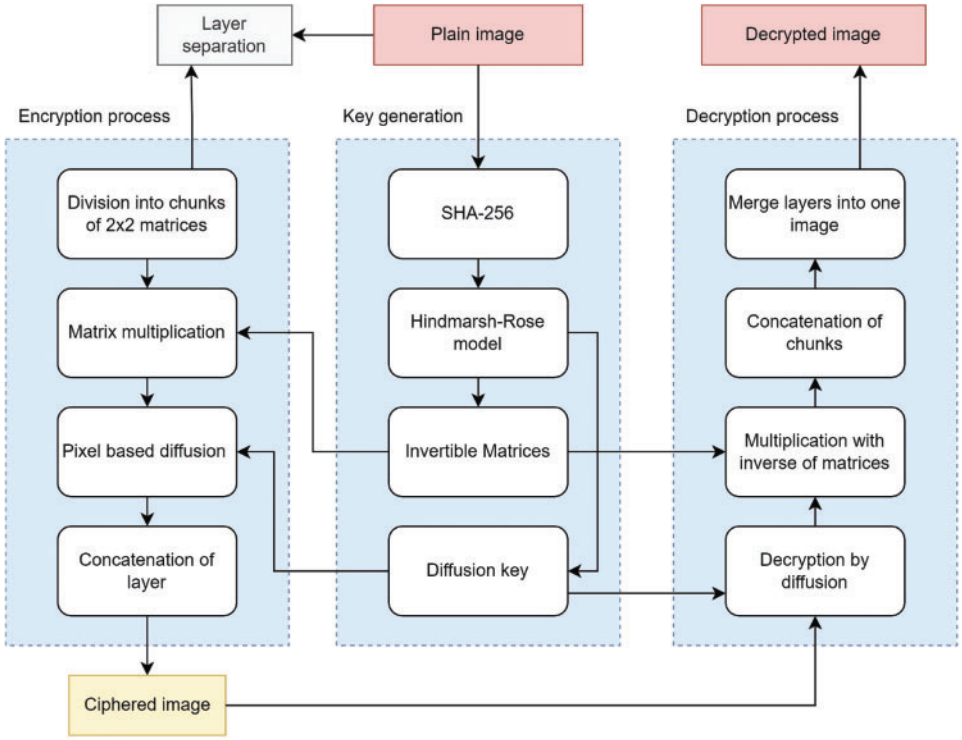

Figure 2: The flowchart of the proposed scheme

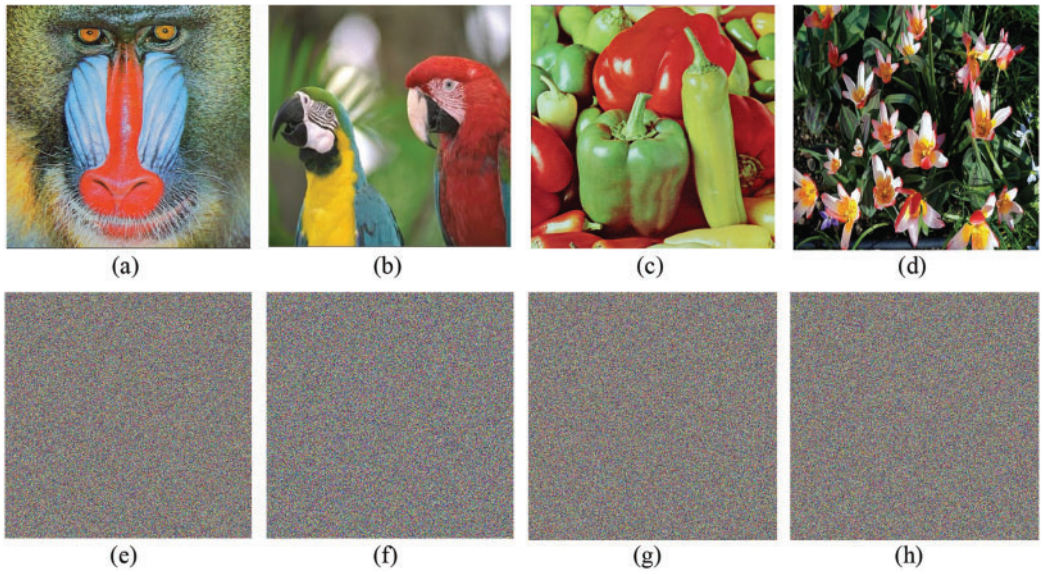

Figure 3: Plain images of (a) Baboon; (b) Parrots; (c) Peppers; (d) Tulip; (e–h) respective cipher images

5 Security Performance Analyses

The security evaluation of any cryptosystem is essential to claim the quality performance of an image encryption scheme. Therefore, to assess the robustness, we analysed several image encryption metrics. The results of several metrics are listed below.

5.1 Histogram

The histogram of an image provides a visual representation of how the image's pixel values are distributed. Plaintext images typically exhibit non-normal distribution shapes in their histograms. The histograms of an encrypted image should be uniformly distributed for higher security. The statistical histograms of Baboon, Parrots, Peppers, and Tulip test images and their enciphered counterparts are displayed in Fig. 4.

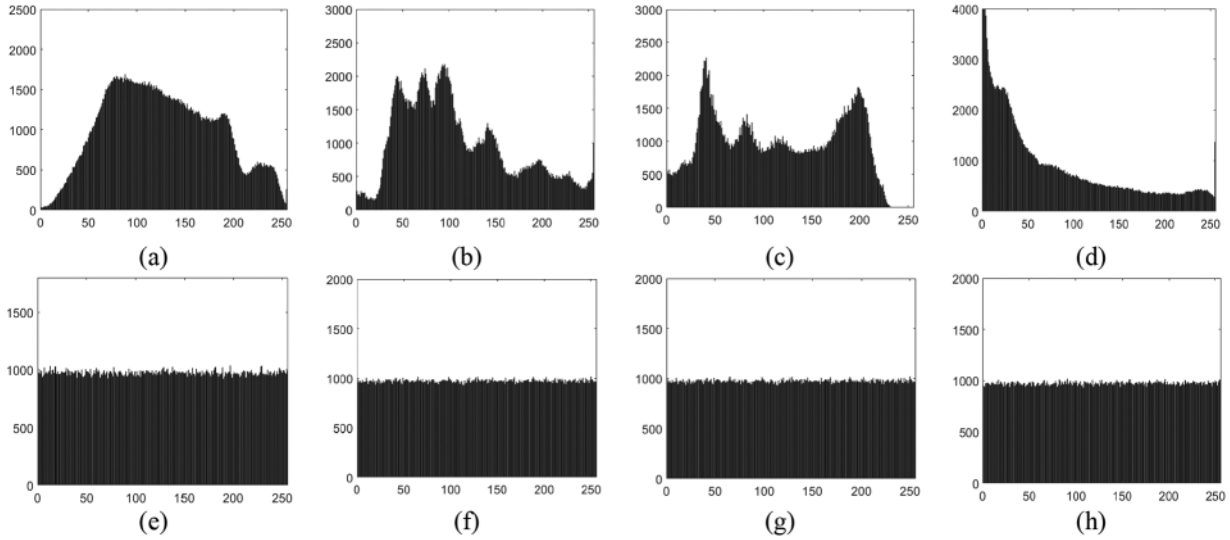

Figure 4: Histogram of Baboon, Parrots, Peppers, Tulip (a–d) original (e–h) encrypted images correspondingly

The horizontal coordinates in Fig. 4 represent pixel value and the vertical coordinate denotes the frequency occurrence of each pixel. The histograms of the encrypted and plaintext versions of the image are very different from one another. The histogram of the enciphered ciphertext image is normally dispersed, even though the histogram of the plain image was not. Consequently, the encrypted image is secure against attacks based on statistical analysis.

5.2 Chi-Square Analysis

Furthermore, we can use the Chi-square test to quantify the histogram's uniformity distribution. The Chi-square χ^2 of an image can be determined as follows:

$$\chi^2 = \sum_{i=1}^{n} (O_i - E_i)^2 / E_i, \tag{5}$$

where n denotes the number of grayscale levels in the image, O_i is the frequency with i-th gray level that has been detected, and E_i is the expected standard frequency with i-th gray level that has been observed for an image with dimensions $M \times N$, $E_i = M \times N \times n$. The critical value for an 8-bit grayscale image ($n = 256$) at a significance level, $\alpha = 0.05$ is $\chi^2(255, 0.05) = 293.2478$. For an enciphered 8-bit

grayscale image, the value must be less than 293.2478. Numerous test images and their enciphered counterparts are used in the test, and the findings are summarized in Table 2.

Table 2: χ^2 results of the proposed scheme and comparative results

Image	χ^2 of cipher image	Ref. [29]	Ref. [17]
Baboon	233.5158	244.7559	245.0137
Parrots	215.4871	–	–
Peppers	222.9162	–	–
Tulip	239.5591	–	–

From Table 2, the Chi-square results of all the enciphered images are smaller than the crucial value. However, the Chi-square estimate of enciphered images produced by our proposed work is lower than that of similarly prepared images from other encryption schemes.

5.3 Correlation Coefficient

There is a strong correlation among neighbouring pixels in meaningful plaintext images. As such, a strong encryption method needs to be able to break the link among adjacent pixels. A correlation coefficient provides a quantitative calculation of the degree to which neighbouring pixels are correlated with one another. In this work, we used the correlation coefficient, a measure for examining the degree to which neighbouring image pixels share common characteristics.

$$E(x) = \frac{1}{N_{xy}} \sum_{i=1}^{N_{xy}} x_i, \tag{6}$$

$$D(x) = \frac{1}{N_{xy}} \sum_{i=1}^{N_{xy}} (x_i - E(x))^2, \tag{7}$$

$$\operatorname{cov}(x, y) = \sum_{i=1}^{N_{xy}} (y_i - E(y))(y_i - E(y)), \tag{8}$$

$$r_{xy} = \operatorname{cov}(x, y) / \sqrt{D(x)} \sqrt{D(y)}, \tag{9}$$

where (x_i, y_i) is a pair of integers representing the average grey amount of a sample of neighbouring pixels in the image, and N_{xy} is the total quantity of sampled pixel bands. Since the r_{xy} correlation coefficient has a smaller absolute value, there is less of a connection between the two sets of pixels. Correlation coefficients for diagonally adjacent pixels in the enciphered image are explained in Table 3.

Table 3: Correlation coefficient of the proposed scheme and comparative results

Image	Direction	Proposed scheme	Ref. [29]	Ref. [30]
Baboon	Horizontal	−0.0009	−0.00007	0.0020
	Diagonal	−0.0010	−0.00007	0.0020
	Vertical	−0.0007	−0.00007	0.0020
Parrots	Horizontal	0.0001	–	–
	Diagonal	0.0008	–	–
	Vertical	−0.0052	–	–

(Continued)

Table 3 (continued)

Image	Direction	Proposed scheme	Ref. [29]	Ref. [30]
Peppers	Horizontal	−0.0078	−0.0046	0.0043
	Diagonal	0.0029	−0.0046	0.0043
	Vertical	0.0011	−0.0046	0.0043
Tulip	Horizontal	0.0030	–	–
	Diagonal	0.0004	–	–
	Vertical	−0.0006	–	–

The comparison outcomes are shown in Table 3. The proposed approach yields good results, especially when compared to state-of-art techniques. In this study, we present a method that utilizes the Hindmarsh Rose model to create confusion and diffusion among pixels.

Fig. 5 plots the distribution of neighbouring pixel values for the Parrots, making it easy to see how their values are related to one another. Fig. 5 shows that, in the original Parrots image, neighbouring points are typically distributed along or around the 45-degree line, signifying that the estimates of nearby pixels are the same or very similar. Yet, there is a significant variance in value between neighbouring pixels, as seen by the fact that the ciphertext image's adjacent points are not centred on the 45-degree line. As a result, the image's pixel correlation is essentially broken by the encryption technique.

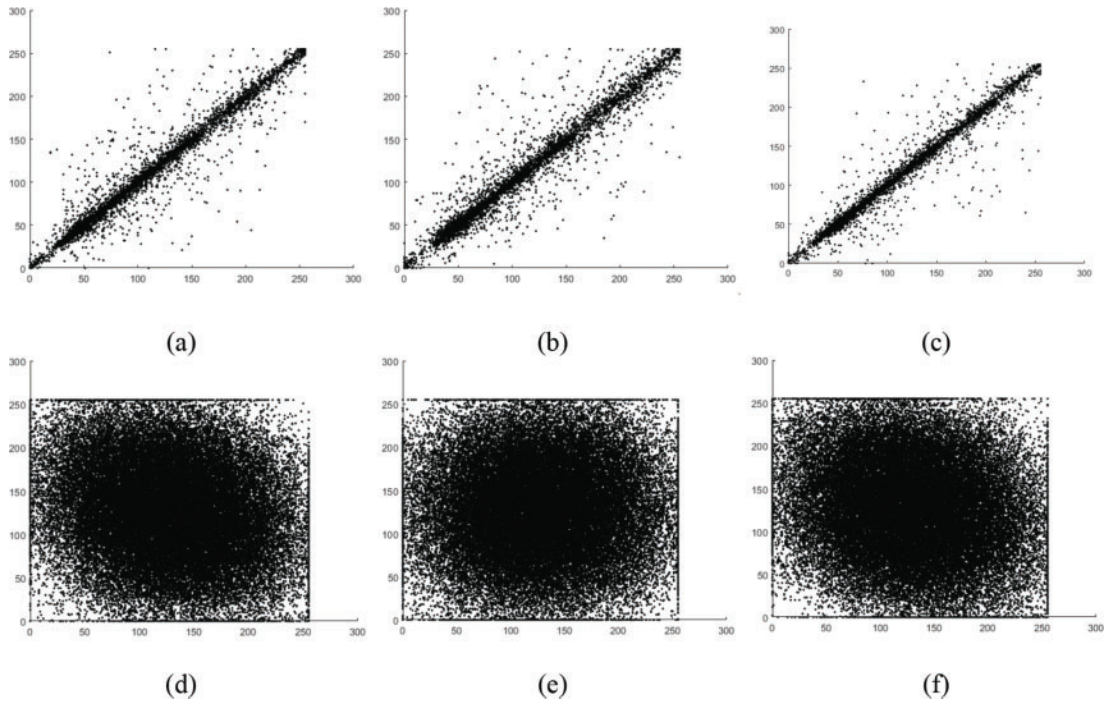

Figure 5: Parrots image correlation diagram (a–c) plain; (d–f) enciphered in horizontal, diagonal, and vertical paths correspondingly

5.4 Entropy

Information entropy can be utilized to calculate how unpredictable or random data is. The greater the information entropy, the more difficult it is to forecast or understand the underlying information. The following formula may be used to determine an information source's entropy:

$$H(S) = -\sum_{i=1}^{n} p_i \log_2(p_i), \tag{10}$$

where $S = s_1, s_2, \ldots, s_n$ is the information source and p_i is the probability that s_i will occur. The maximum information entropy principle states that an information source has the highest possible entropy, or $\log_2(n)$, when all possible states s_i have the same probability $p_i = (1/n)$. An 8-bit grayscale image's data source has 256 grey levels, making $n = 256$. As $\log_2(256) = 8$ is the highest possible entropy for a grayscale image, this is the case. Hence, the larger the uncertainty and the significant the robustness of an enciphered image, the nearer its information entropy is to 8. Table 4 shows the entropy of encrypted examples of typical test images using this approach and other previously published schemes.

Table 4: Information entropy analysis results

Image	Proposed scheme	Ref. [20]	Ref. [5]
Baboon	7.9999	7.9971	7.9970
Parrots	7.9998	–	–
Peppers	7.9989	7.9970	7.9973
Tulip	7.9997	–	–

The results demonstrate that ciphertext image information entropy is quite near to the maximum value and hence the proposed scheme is secure against entropy attack.

5.5 Differential Attack Analysis

The strong sensitivity of the ciphertext to the plaintext and the secret keys is a feature of an effective encryption algorithm. A comparison of the enciphered image's sensitivity to the original image or secret keys can be carried out with either NPCR or UACI. Mathematically, NPCR and UACI are written as:

$$D(i,j) = \begin{cases} 1, if\ C(i,j) \neq C'(i,j), \\ 0, if\ C(i,j) = C'(i,j), \end{cases} \tag{11}$$

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{12}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| \frac{C(i,j) - C'(i,j)}{255} \right| \times 100\%, \tag{13}$$

where M and N refer to the image's row and column coordinates. The sensitivity of the encryption technique is relative to the square root of the product of NPCR and UACI. An NPCR of 99.6094% and a UACI of 33.4635% are considered good for image encryption.

After comparing the UACI and NPCR values of two different enciphered images for the key sensitivity study, we found that the respective encryption keys differed by just one parameter on the order of 10^{15}. Tabulated below are the outcomes of the experiments. Experimental findings

demonstrate that UACI and NPCR values are close to the ideal values, showing that the cryptosystem is highly sensitive to the specifics of every key parameter. The proposed scheme has higher key sensitivity than the results from [29,30]. Table 5 summarizes the findings from the experiments.

Table 5: NPCR and UACI analysis of offered scheme and comparative results

Image	Proposed		Ref. [29]		Ref. [30]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Baboon	99.63	33.25	99.6399	33.3027	98.0103	31.1886
Parrots	99.68	33.58	–	–	–	–
Peppers	99.59	34.71	99.6185	33.4211	99.9664	35.6275
Tulip	99.71	33.99	–	–	–	–

5.6 Key Space Analysis

Through, key space analysis, one can analyse the total number of possible keys. In this study, the parameters and starting results of the chaotic model are the original keys to the algorithm. Eleven parameters of double precision $\{a,\ b,\ c,\ d,\ r,\ s,\ x_0, x(0), y(0), z(0),\ I_{ext}\}$ make up the key set if the system parameter is ignored. There are fifteen distinct binary options for each parameter. This results in a total key space of $10^{15*11} = 10^{165} > 2^{249}$. According to [29], an encryption algorithm is considered secure if its key space is larger than 2^{100}. Hence, the proposed technique has a necessarily large key space to resist brute-force attacks.

5.7 MSE and PSNR

In evaluating our algorithm's efficacy, we utilize MSE and PSNR. The MSE shows how far off the target image is from the original. MSE is measured as:

$$MSE = \frac{1}{M_1 \times M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} [I_0(i,j) - I_e(i,j)]^2, \tag{14}$$

where M_1 denotes the row number and M_2 denoted the column number, $I_0(i,j)$ is the value of the plain-image pixel at the position (i,j), and $I_e(i,j)$ is the value of the enciphered image pixel at the position (i,j). PSNR is written as:

$$PSNR = 10 \times \log_{10} \left[\frac{I_{\max}^{\ 2}}{MSE} \right], \tag{15}$$

where $I_{\max}$ is the highest possible pixel quantity in the image. When assessing the encrypted version of an image to the original, the PSNR should be low. Images of Baboon, Parrots, Peppers, and Tulip are encrypted, and the PSNR (dB) of these encrypted images is calculated to compute the quality of the encryption. MSE and PSNR values are illustrated in Table 6. From the Table, it is evident that the proposed scheme is more secure than another encryption scheme.

5.8 Robustness Analysis

While transmitting encrypted images, a good encryption technique should be able to deal with a certain amount of data loss. A visually recognizable decrypted image may be recovered even when noise or data loss corrupts the encrypted image, demonstrating the algorithm's resilience.

Table 6: MSE and PSNR analysis for proposed scheme and comparative results

Image	Proposed		Ref. [29]		Ref. [30]	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Baboon	9308.1	7.9910 dB	7188.3	9.5645 dB	7200.6	9.5571 dB
Parrots	9567.8	8.6561 dB	–	–	–	–
Peppers	8288.5	7.0024 dB	8199.6	8.9929 dB	8093.0	9.0497 dB
Tulip	7685.6	9.0078 dB	–	–		–

To evaluate the algorithm's robustness against data loss, we first encrypt a 256 × 256 image in the top left corner, then divide it into 32 × 32, 64 × 64, and 128 × 128 sub-blocks and decode each one separately. Fig. 6 depicts the decryption effect. The experimental findings demonstrate that the method is even capable of successfully retrieving the plain image even when the sliced region is as large as 128 × 128. The technique described in [30] can only handle a maximum data loss size of 8 × 16 in enciphered images, in contrast. Using the techniques described in [30], we find that when our enciphered image has a data loss with dimensions 128 × 128, the deciphered image is identical to the enciphered image with a data loss of 8 × 16. Our technique outperforms the scheme proposed in [30] in terms of resilience to data loss.

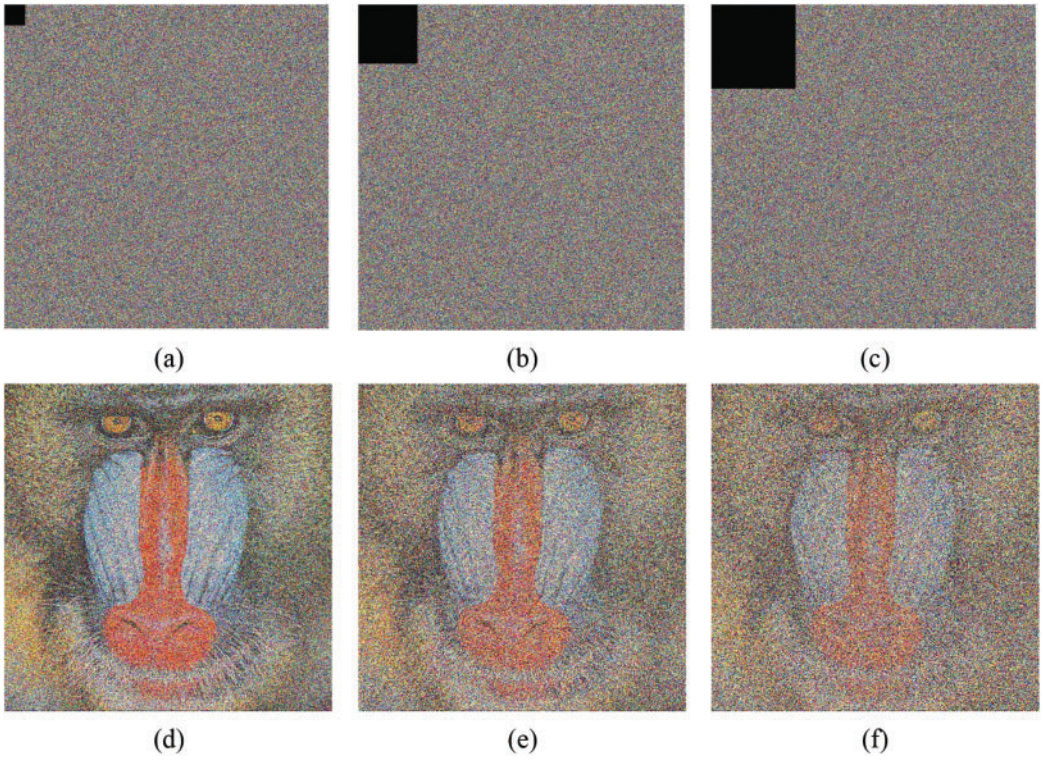

Figure 6: Cipher image of Baboon with a black chunk of (a) 32 × 32; (b) 64 × 64; (c) 128 × 128; (d–f) respective decrypted images

5.9 Time Complexity Analysis

The proposed approach encrypts data in three distinct steps: generating Hindmarsh-Rose chaotic secret key streams, encryption of pixels using invertible matrices, and pixel diffusion carried by bitwise XOR operation. As part of the algorithm's time-cost analysis, we encrypt and decrypt a 256-by-256 grayscale Baboon image. Table 7 displays the average encryption and decryption times (in seconds) from some different studies. Table 7 also includes statistics on the time cost of several chaos-based algorithms taken from recently published work. The outcomes show that the proposed method is quicker at both encrypting and decrypting than the methods discussed in [30,31].

Table 7: Time comparison of the proposed scheme with already published work

Phase	Proposed	Ref. [30]	Ref. [31]
Encryption	0.9701 s	12.6500 s	14.8401 s
Decryption	0.7814 s	12.8410 s	14.9266 s

5.10 Classical Cryptanalysis Attack

The strength of the proposed encryption scheme can be measured by evaluating it against classical cryptanalysis attacks. When the system is subjected to the chosen plaintext or chosen ciphertext attack then the attacker might try to insert some images trying to recover the private keys from the system. As the proposed encryption scheme utilized the algorithm of SHA-256 based on the input of the algorithm, therefore, the output against each image would be different. Therefore, the proposed structure can resist all types of classical attacks due to its nature of the complex design.

6 Conclusion

In this study, we present a novel three-dimensional Hindmarsh-Rose model-based cryptosystem that demonstrates significant chaotic behaviour across a wide range of parameters. The proposed encryption method is mainly based on chaos theory and offers suitability for real-time encryption. To assess the effectiveness of the model, we utilized standard measures commonly employed in chaos theory. During the testing phase of our proposed scheme, we observed robust chaotic behaviour across various parameter values. Furthermore, we employed the chaotic map to create a faster and more secure image encryption technique. This proposed image encryption approach combines multiplication and diffusion operations, effectively merging permutation and substitution into a single step. As a result, the proposed scheme achieves efficiency and enhanced security compared to the conventional encryption algorithms. Performance analysis of the proposed encryption algorithm demonstrates that it satisfies numerous ideal values across different measures. Moreover, the algorithm successfully passes all security tests along with low computational complexity. We tested the proposed image encryption technique using extensive simulation and experimental tests, which confirmed its suitability for real-time applications. Additionally, we plan to apply the proposed method to encrypt audio and video data in the future. Our forthcoming research will focus on evaluating the effectiveness of the proposed encryption method on videos and audio.

Acknowledgement: The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work under the Research Groups Funding Program Grant Code (NU/RG/SERC/12/3).

Funding Statement: The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work under the Research Groups Funding Program Grant Code (NU/RG/SERC/12/3).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Barrio, S. Ibáñez and L. Pérez, "Hindmarsh–Rose model: Close and far to the singular limit," *Physics Letters A*, vol. 381, no. 6, pp. 597–603, 2017.
[2] A. Atangana and I. Koca, "Analytical and numerical investigation of the Hindmarsh-Rose model neuronal activity," *Mathematical Biosciences and Engineering*, vol. 20, no. 1, pp. 1434–1459, 2023.
[3] S. Zhang, L. Liu and H. Xiang, "A novel plain-text related image encryption algorithm based on LB compound chaotic map," *Mathematics*, vol. 9, no. 21, pp. 1–25, 2021.
[4] D. S. Malika and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps," *Mathematics and Computers in Simulation*, vol. 178, pp. 646–666, 2020.
[5] I. Ö. Ztürk and R. Kılıç, "Utilizing true periodic orbits in chaos-based cryptography," *Nonlinear Dynamics*, vol. 103, pp. 2805–2818, 2021.
[6] C. X. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, pp. 29–37, 2012.
[7] S. Zhu, G. Wang and C. Zhu, "A secure and fast image encryption scheme based on double chaotic S-boxes," *Entropy*, vol. 21, pp. 790, 2019.
[8] X. Chai, J. Fu, Z. Gan, Y. Lu and Y. Zhang, "An image encryption scheme based on multi-objective optimization and block compressed sensing," *Nonlinear Dynamics*, vol. 108, pp. 2671–2704, 2022.
[9] G. Ye, M. Liu and M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria Engineering Journal*, vol. 61, pp. 6785–6795, 2022. https://doi.org/10.1016/j.aej.2021.12.023
[10] G. Ye, H. Wu, M. Liu and Y. Shi, "Image encryption scheme based on blind signature and an improved lorenz system," *Expert Systems with Applications*, vol. 205, pp. 117709, 2022. https://doi.org/10.1016/j.eswa.2022.117709
[11] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.
[12] A. Ouannas, A. A. Khennaoui, X. Wang, V. T. Pham, S. Boulaaras *et al.,* "Bifurcation and chaos in the fractional form of Hénon-Lozi type map," *The European Physical Journal Special Topics*, vol. 229, pp. 2261–2273, 2020.
[13] A. Ouannas, A. A. Khennaoui, T. E. Oussaeif, V. T. Pham, G. Grassi *et al.,* "Hyperchaotic fractional Grassi–Miller map and its hardware implementation," *Integration*, vol. 80, pp. 13–19, 2021.
[14] A. A. Khennaoui, A. Ouannas, S. Boulaaras, V. T. Pham and A. T. Azar, "A fractional map with hidden attractors: Chaos and control," *The European Physical Journal Special Topics*, vol. 229, pp. 1083–1093, 2020.
[15] L. Liu and S. Miao, "A new simple one-dimensional chaotic map and its application for image encryption," *Multimedia Tools and Applications*, vol. 77, pp. 21445–21462, 2018.
[16] Y. Li, X. Li and X. Liu, "A fast and efficient hash function based on generalized chaotic mapping with variable parameters," *Neural Computing and Application*, vol. 28, pp. 1405–1415, 2016.
[17] W. Yu and T. Yu, "Analysis of chaotic characteristics of trigonometric function system," *Modern Physics Letters B*, vol. 34, pp. 2050210, 2020.
[18] A. N. Elghandour, A. M. Salah, Y. A. Elmasry and A. A. Karawia, "An image encryption algorithm based on bisection method and one-dimensional piecewise chaotic map," *IEEE Access*, vol. 9, pp. 43411–43421, 2021.

[19] T. Gopalakrishnan and S. Ramakrishnan, "Image encryption using hyper-chaotic map for permutation and diffusion by multiple hyper-chaotic maps," *Wireless Personal Communications*, vol. 109, pp. 437–454, 2019.
[20] R. Zahmoul, R. Ejbali and M. Zaied, "Image encryption based on new beta chaotic maps," *Optics and Lasers in Engineering*, vol. 96, pp. 39–49, 2017.
[21] M. Alawida, A. Samsudin, J. S. The and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2017.
[22] E. G. Nepomuceno, L. G. Nardo, J. A. Garcia, D. N. Butusov and A. Tutueva, "Image encryption based on the pseudo-orbits from 1D chaotic map," *Chaos*, vol. 29, pp. 061101, 2019.
[23] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Information Science*, vol. 520, pp. 46–62, 2020.
[24] H. Huang, S. Yang and R. Ye, "Efficient symmetric image encryption by using a novel 2D chaotic system," *IET Image Processing*, vol. 14, pp. 1157–1163, 2020.
[25] S. Askar, A. Karawia, A. A. Khedhairi and F. A. Ammar, "An algorithm of image encryption using Logistic and two-dimensional chaotic economic maps," *Entropy*, vol. 21, pp. 44, 2019.
[26] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, *et al.,* "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020.
[27] Q. Lu, C. Zhu and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-Box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.
[28] S. Zhu and C. Zhu, "Security analysis, and improvement of an image encryption cryptosystem based on bit plane extraction and multi chaos," *Entropy*, vol. 23, pp. 505, 2021.
[29] S. Zhu and C. Zhu, "An efficient chosen-plaintext attack on an image fusion encryption algorithm based on DNA operation and hyperchaos," *Entropy*, vol. 23, pp. 804, 2021.
[30] S. Zhu, X. Deng, W. Zhang and C. Zhu, "Image encryption scheme based on newly designed chaotic map and parallel DNA coding," *Mathematics*, vol. 11, pp. 231, 2023.
[31] H. Zang, M. Tai and X. Wei, "Image encryption schemes based on a class of uniformly distributed chaotic systems," *Mathematics*, vol. 10, no. 7, pp. 1–27, 2022.
[32] S. Zhu, X. Deng, W. Zhang and C. Zhu, "A new one-dimensional compound chaotic system and its application in high-speed image encryption," *Applied Sciences*, vol. 11, no. 23, pp. 11206, 2021.