Int. J. Nonlinear Anal. Appl. 13 (2022) 1, 2179-2194
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.5914

# Efficient image encryption via chaotic hight algorithm

Woud M. Abed[a,*]

[a]Department of Basic Sciences, College of Dentistry, University of Baghdad, Iraq

(Communicated by Madjid Eshaghi Gordji)

**Abstract**

This paper is devoted to introducing a new three dimensions hyperchaotic system and adapting it to enhance the Hight algorithm. The proposal hyperchaotic system with one equilibrium point is mainly derived from the Lorenz system, which we called (3D-NSC). The dynamic analysis of 3D-NSC presents some properties such as; stability of symmetric equilibria; phase diagram, bifurcation and Lyapunov exponents (LE), which are all investigated analytically and numerically. Also, the circuit design of the 3D-NSC is introduced with some properties. The proposed system is occupied with improving the Hight algorithm. The main propose system is to create a key schedule for the chaotic Hight algorithm. This system is then applied to encrypt different images types. Our proposed system showed high encryption efficiency compared to systems, based on some performance analyzes such as; histogram, pixel change rate (NPCR), standardized variable mean intensity (UACI), pixel correlation, and entropy.

*Keywords:* Chaotic system, Hyperchaotic, Image encryption, Hight algorithm, Circuit Design.

## 1. Introduction

In recent years, the means of communication via the internet of various kinds becomes a reality for our lives and becomes a means of transmitting and receiving all information. Therefore, preserving this information is necessary. In other words, the confidentiality of information through the transmission of data is a significant issue. As a consequence, many researchers and security agencies have introduced many encryption methods such as RSA, Data Encryption Standard (DES), and Advanced Encryption Standard (AES), which are considered the traditional methods and inadequate for securing. This is due to their distinguishing features, such as including bulk data capacity,

*Corresponding author
*Email address:* wood.majid@codental.uobaghdad.edu.iq (Woud M. Abed)

*Received:* September 2021 *Accepted:* November 2021

high redundancy [20]. After that, several researchers introduced many various algorithms which are stronger more than its predecessor from the traditional algorithm, such as, compressive sensing [40]; wavelet transmission [34]; affine transformation[25]; neural network [23]; fractal theories [4, 5, 3], and chaotic algorithms [14, 36, 15]. Virtually, chaotic systems in cryptography are considered more efficient than the other method. Chaotic systems have randomness, complexity, and mixing that achieves Shannon's principles of cryptography, diffusion and confusion [24, 31].

In the 1970s mathematicians used a new term for systems that are complex and unpredictable called dynamical systems. As these systems contain some characteristics, including ergodicity, and a sensitivity dependence on initial values and parameters. These chaotic systems have been used and become known to many physicists and mathematicians, the most prominent of these scientists Poincare [29].

Two types of chaotic systems, a discrete-time and continuous-time systems. The discrete-time chaotic systems can be described by difference equations, whereas the continuous-time chaotic systems can be described by partial differential equations and ordinary differential equations [32]. Chaotic systems have some features such as unpredictability, which made them useful for other fields such as information theory, engineering, communications, power system protection, etc. [26, 27].

Chaotic systems have been used in cryptographic systems, and the essential reason is the extreme chaoticity and high randomness, which is mainly used in the formation of strong keys, therefore many researchers have introduced several algorithms with fast performance and high security. Some researchers such as, Liu et al. [21], Hua et al. [14], Diab et al. [10], and Koppu et al. [19] introduced new algorithms for image encryption based essentially on 2- dimensions chaotic maps. Others continued to provide encryption algorithms based mainly on chaotic systems, for example, Hayder et al. [28], Hua, Zhongyun, et al. [16] and Cao et al. [9]. In 2019, Alawida, M. et al. [1] presented a new proposed of image encryption based on hybridizing digital chaos and finite state machine. In the same year, Ali, D. S.[2] proposed a new 2D- hyperchaotic map called Henon, logistic, iterative chaotic map with infinite collapse (ICMIC) maps (2D-HLCM), which was adopted to design a new encryption algorithm for an image. Khan, M. et al. [17] introduced a new technique for image encryption essentially based on a hybrid method that combines chaotic systems and Brownian motion. In 2021, Was, M. T. et al. [3] proposed a novel algorithm called the image splitting algorithm based mainly on three chaotic maps are combined together to generate a new 2D- chaotic map called 2D-LCHM. Additionally, several investigators proposed encryption algorithms based on a 3D-chaotic system, such as Farhan et al. [11] presented a new proposed for image encryption based on 3D chaotic maps containing a unique feature of repeatedly crossing inside and outside a cylinder. In 2021 Yan, W. et al. [37] introduced a new encryption algorithm based on a novel 3D-infinite collapse map (3D-ICM). In the same year, Alwan, N. A. et al. [6] proposed a chaotic RSA encryption algorithm based essentially on a 3-D chaotic dynamic system derived from 3D-Memristor and 3D-Sprott's chaotic systems. Asl, A. M. et al. [7] proposed an image encryption system for scale-invariant digital colour using a 3D-modular chaotic system.

In this effort, a three-dimensional hyperchaotic system derived from the Lorenz system, called (3D-NSC), which has highly distributed and complex behavior, and better ergodicity is proposed. We also designed an electronic circuit for our chaotic system using the program proteus design suite. Through the 3D-NCS, the secret key's initial values are produced; it is then used to produce a pseudo-random number generator (PRNG) which is used to generate a key schedule for the hight algorithm that realized confusion and diffusion. Our encryption system is used to encrypt multiple types of colour and grayscale images. The proposed system is analyzed to evaluate its performance using much analytics such as; histogram, correlation pixels, and Shannon entropy analyses. The analysis results from the proposed encryption system have high security and high efficiency. The

remainder of this paper is organized as follows. The design and the performance of the 3D-NCS, such as a phase diagram, bifurcation and LE, are described in section 2. AS well, the circuit design is also is presented in this section. Section 3 introduced the encryption system includes the hight encryption algorithm traditional, and algorithm of hight encryption developed. Simulation results and an analysis of the security are introduced in Section 4. Then in Section 5 the conclusion of this article.

## 2. A new 3-dimensions chaotic system and its properties

The new 3-dimensions chaotic system (3D-NCS) derived from Lorenz system [22] is defined by the following differential equation:

$$\begin{aligned} \dot{x} &= cy - x - bz, \\ \dot{y} &= axz - xy - bx, \\ \dot{z} &= xy - bz, \end{aligned} \tag{2.1}$$

where $x, y, z$ and $a, b, c$ are state variables, parameters, respectively.
Initial values of the system are $x(0) = 0, y(0) = 0, z(0) = 0$, and the parameters values intervals are $a \in (10, 100), b \in (30, 150)$, and $c \in (10, 100)$.

### *2.1. Equilibrium point of 3D-NCS*

Th equilibria point of 3D-NCS, can be obtained by setting the right-hand side of (2.1) equals zero.

$$\begin{aligned} cy - x - bz &= 0, \\ axz - xy - bx &= 0, \\ xy - bz &= 0, \end{aligned} \tag{2.2}$$

After simple arithmetic, the equilibrium point are $E\left(\frac{b(b+1)}{a}, b^2, \frac{b^2(b+1)}{a}\right)$, where $a > 0$. Via Jacobian matrix can be investigated about the local behaviour of the system 3D-NCS around the equilibrium point:

$$Jac(x, y, z) = \begin{bmatrix} -1 & c & -b \\ az - y - b & -x & ax \\ y & x & -b \end{bmatrix} \tag{2.3}$$

The Jacobian matrix for equilibrium point $E$ become:

$$Jac(E) = \begin{bmatrix} -1 & c & -b \\ b^3 - b & -\frac{b(b+1)}{a} & b(b+1) \\ b^2 & \frac{b(b+1)}{a} & -b \end{bmatrix} \tag{2.4}$$

The eigenvalue of 3D-NCS is obtained from $\det(\lambda I - Jac(E)) = 0$, where det refers to matrix determinant, and $I$ refers to identity matrix. The characteristic polynomial of $E$ is obtained from the Jacobian matrix for equilibrium point $E$ is:

$$\lambda^3 + m_1\lambda^2 - m_2\lambda - m_3 = 0 \tag{2.5}$$

where $m_1 = \frac{(a-b+ab-b^2)}{a}, m_2 = \frac{b-ab-ab^3+3b^2+3b^3+b^4-abc+ab^3c}{a}$, and $m_3 = \frac{2b^2+4b^3+3b^4-b^6-ab^2c+ab^3c+2ab^4c}{a}$, where $a > 0$.
Then the eigenvalues of the above characteristic polynomial are:

for $E(226.5, 22500, 33748.5)$: where $a = 100, b = 150$, and $c = 100$;

$$\lambda_1 = 18209.12;$$
$$\lambda_2 = -18627.410;$$
$$\lambda_3 = 40.78;$$

for $E(755, 22500, 112495)$: where $a = 30, b = 150$, and $c = 30$;

$$\lambda_1 = -12434.34;$$
$$\lambda_2 = 7940.27;$$
$$\lambda_3 = 3588.067;$$

We have complex eigenvalues where values $a \in (10, 19)$, and $c \in (10, 19)$ for example $E(2059.09, 22500, 306804.54)$, where $a = 11, b = 150$, and $c = 11$;

$$\lambda_1 = -13649.086 + 0i;$$
$$\lambda_2 = 5719.497 + 6583.578i;$$
$$\lambda_3 = 5719.497 - 6583.578i;$$

## 3. Dynamical Analysis of the 3D- new chaotic system

In this section, we introduced the performance of (2.2) via an phase diagram, bifurcation and expansion Lypencove (LE) shows in Figures (1, 2, 3), respectively.

### *3.1. Phase diagram*

A dynamic attractor system is to draw a path for the system via a set of points that describe the behaviour of the system and track its motion, starting with the initial point and the effect of the parameters. The parameter set of 3D-NCS a,b, and c to guarantee the trajectory maximum range spread, where $a \in (10, 100)$, $a \in (30, 150)$, and $a \in (10, 100)$. For the initial variables of 3D-NCS with one equilibrium given as $(x_0, y_0, z_0) = (0, 0, 0)$. Figure 1 (a)-(d) shows the attractor of x-y-z, x-y ,x-z, and y-z, of 3D-NCS, respectively. where the initial variables is $(0, 0, 0)$, shows the attractor of where parameters are $a = 100; b = 150$, and $c = 100$.

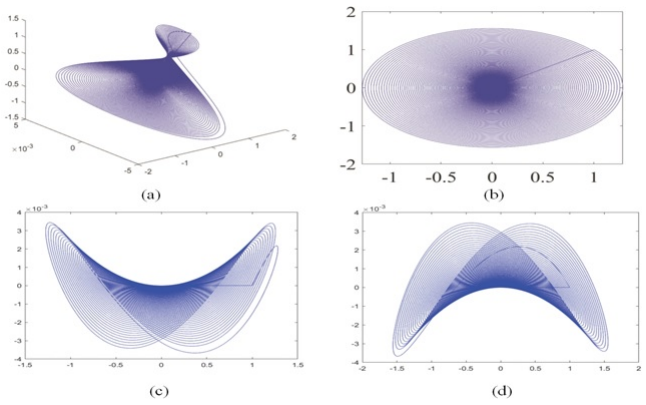


Figure 1: Different orientations on 3D-NCS attractor for the initial variables $(0, 0, 0)$, and the parameters values of a; b and c are: (a) 100; 150, and 100, respectively. (a)x-y-z attractor; (b) x-y attractor; (c) x-z attractor; and (d) y-z attractor.

### *3.2. Chaotic behavior using Bifurcation and Lyapunov exponents*

There are many measures to describe the chaotic dynamic systems, the most famous are bifurcation and Lyapunov exponents. The bifurcation is a study of changes in the qualitative or topological structure of a chaotic system that refers to the phenomenon of a system exhibiting new behavior as varying parameters.

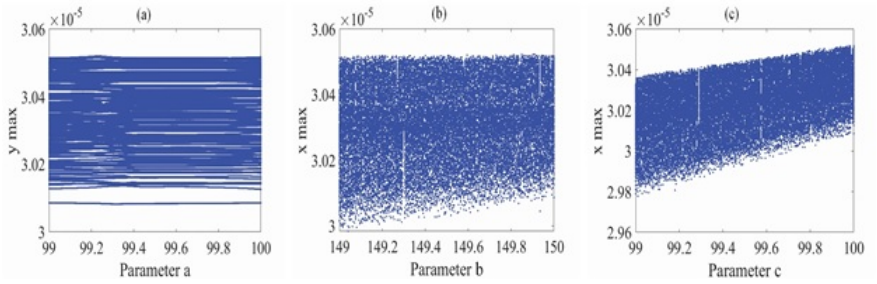


Figure 2: The bifurcation diagram of 3D-NCS for the initial variables $(0, 0, 0)$, and the parameters values of a; b and c are: (a) when $b = 150, c = 100$, and $a \in [99 : 100]$ step $= 0.01$, respectively, (b) when $a = 100, c = 100$, and $b \in [149 : 150]$ step $= 0.01$, respectively, and (c) $a = 100, b = 150$, and $c \in [99 : 100]$ step $= 0.01$, respectively.

To describe the dynamical behavior of 3D-NCS, used Lyapunov exponents (LE), which is the rate that measures the divergence or convergence between two neighboring trajectories. LE can be defined mathematically as [33]:

$$\lambda \cong \frac{1}{t} \ln \frac{\| \delta x(t) \|}{\| \delta x(0) \|} \tag{3.1}$$

where $\frac{\|\delta x(t)\|}{\|\delta x(0)\|}$ is the distance between two neighboring trajectories.
Any system is called chaotic if the LE includes at lest one positive trajectory, or hyperchaotic if LE includes two or more positive trajectory [33].
Figure 3 depicts the LE of 3D-NCS of some states, where the parameters are set as $a = 100$, $c = 100$, and $30 \leq b \geq 150$, and the initial variables are $(x, y, z) = (0, 0, 0)$. This figure clearly shows the dynamical system of 3D-NCS is hyperchaotic. In Figure 3(a) the first LE (blue line) is positive, the second LE (red line) is positive with large values, and the third LE (yellow line) is negative, in the same Figure 3(b) shows the first and second LE (blue red line) is zero, resectovely, while the third LE is negative, in the range 0.2 to 0.68. whereas in the range 0.68 to 1, the values of the first and second LE are rise up while the third LE continues to be negative.

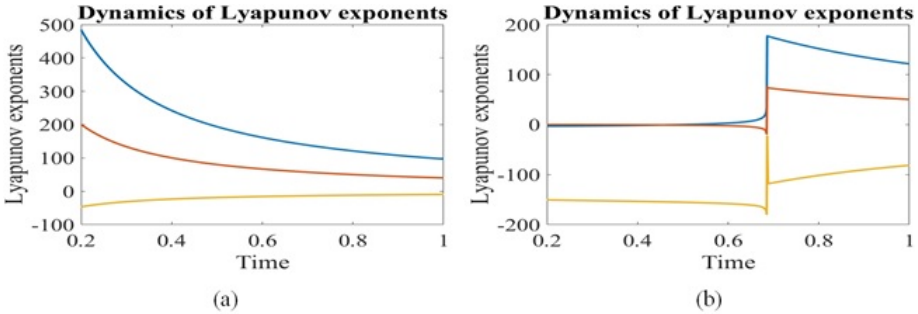


Figure 3: The Lyapunov exponents of 3D-NCS for the initial variables $(0, 0, 0)$, and the parameters values of a; b and c are: (a) when $a = 100, b = 150$, and $c = 100$, respectively, and (b) when $a = 100, b = 300$, and $c = 100$, respectively.

## 4. Analog Circuit Design

Many chaotic circuits have recently been created to induce chaos. The ability to synchronize chaotic circuits offers up a variety of uses for them, including signal masking and communication security. A circuit diagram for the proposed driven is built using system (2.2), as illustrated in Figure 4. The circuit is mostly made up of 5 op-amp (TL084ACN), 3 multipliers, 3 capacitors, and 12 Resistors.

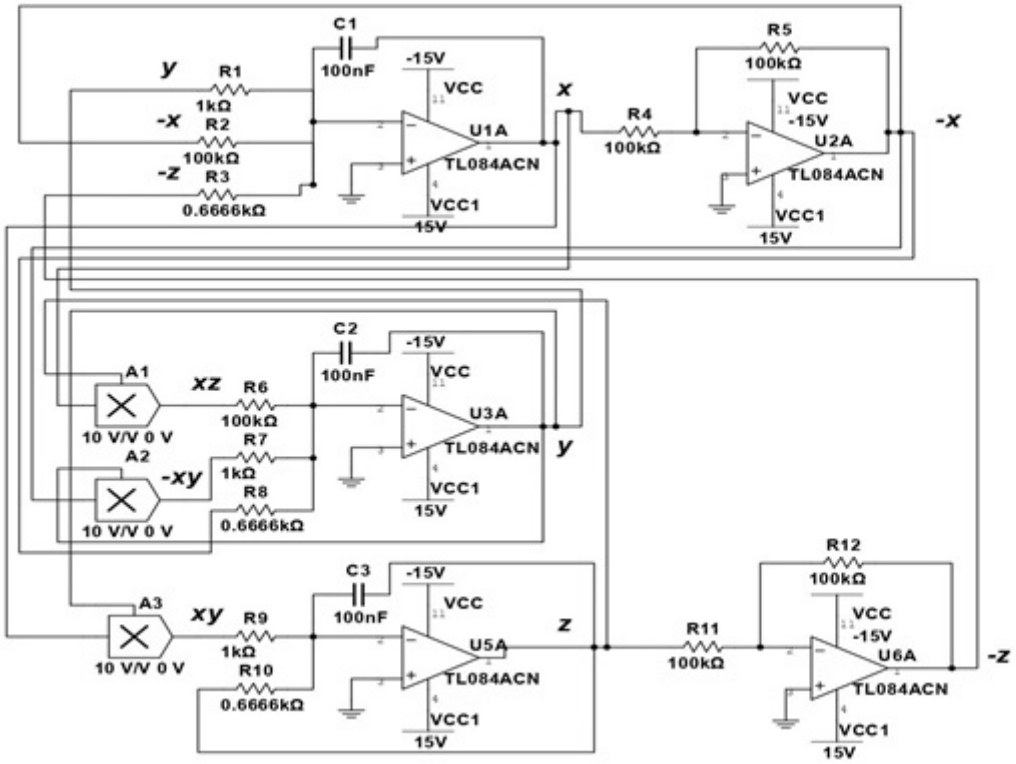


Figure 4: Circuit design of 3D-NCS.

According to the Figure 4, one gets the state equation as follows:

$$\begin{aligned}
\frac{\mathrm{dx}}{\mathrm{dt}} &= \frac{1}{C_1}\left(\frac{y}{R_1} - (\frac{x}{R_2})(\frac{R_5}{R_4}) - (\frac{z}{R_3})(\frac{R_{12}}{R_{11}}\right) \\
\frac{\mathrm{dy}}{\mathrm{dt}} &= \frac{1}{C_2}\left(\frac{\mathrm{xz}}{10\ \ R_6} - \left(\frac{\mathrm{xy}}{10\ \ R_7}\right)\left(\frac{R_5}{R_4}\right) - \left(\frac{x}{R_8}\right)\left(\frac{R_5}{R_4}\right)\right) \\
\frac{\mathrm{dz}}{\mathrm{dt}} &= \frac{1}{C_3}(\frac{\mathrm{xy}}{10\ \ R_9} - \frac{z}{R_{10}})
\end{aligned} \tag{4.1}$$

Comparing equation (2.1) with the proposed chaotic map, one gets $R_1 = R_7 = R_9 = 1k\Omega$, $R_4 = R_5 = R_{11} = R_{12} = 100k\Omega$, and $R_3 = R_8 = R_{10} = 0.6666k\Omega$, where $C_1 = C_2 = C_3 = 100$nf. According to Figure 1, the circuit implementation results of the proposed analog circuit system's simulation results are provided here by the Multisim 12 software and implemented on a computer with specifications Core i3-2.00 GHz, Intel CPU, and 4 GB RAM. Figures 6( a-c) shows the simulation results of the chaotic map's suggested circuit's attractors. the time domain plots of x, y; z chaotic signals are shown in Figure 6 (a-c).

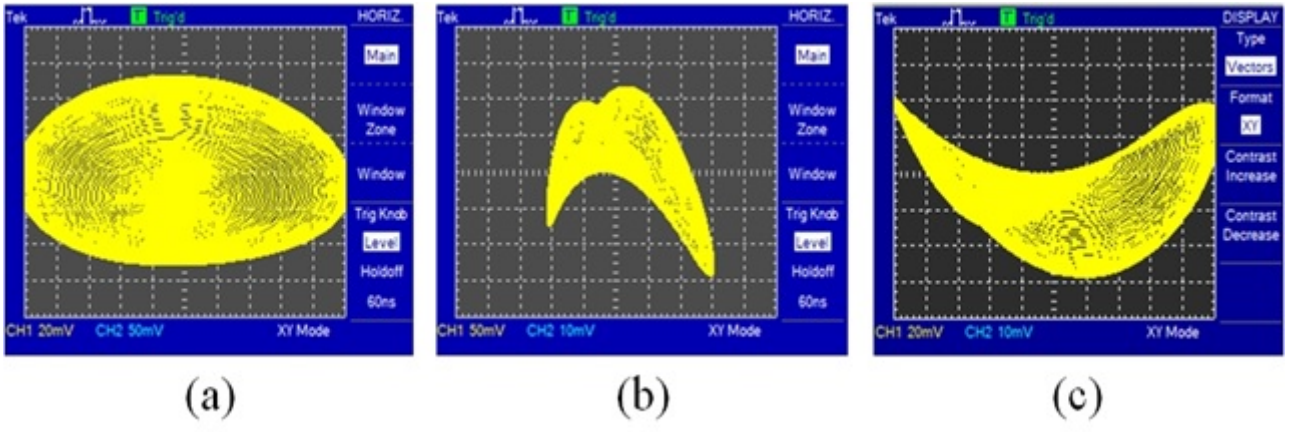


Figure 5: The attractors of the proposed chaotic map (a) xy, (b) xz, and (c) yz.

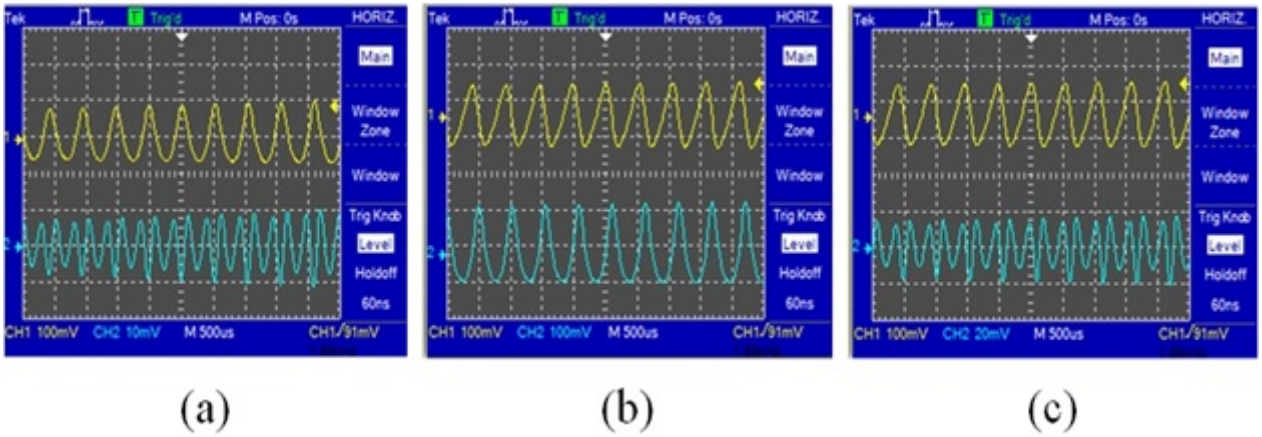


Figure 6: Time domain of :(a)xy, (b) xz, and (c) yz.

## 5. Encryption system

One of the most important security mechanisms is the Hight encryption algorithm for encrypting images or text compared with the other block algorithm such as AES. This section introduced a new proposed for image encryption based on the enhancing of the Hight encryption algorithm for 3D-NCS which is called the enhanced chaotic Hight encryption algorithm (ECHE). For more details about the original algorithm of Hight, we refer the reader to see [13, 18].

### *5.1. The proposed chaotic Hight algorithm cryptosystem*

This section, introduced the improved Hight algorithm based on the 3D-NCS, we called it, chaotic Hight algorithm (CHA). Before that 3D-NCS is used to generate PRNG sequence, which is adapted to generate the chaotic key schedule (CKS). S-box will be the key schedule of the (CHA).

#### *5.1.1. Design a new Key schedule of (CAH)*

This part introduced a new algorithm to generate a chaotic key schedule (CKS) for (CHA) based on 3D-NCS.

*(a) Pseudo-random number generator based on the 3D-NCS*

One of the most important applications that use chaotic systems is encryption, which is used to generate of pseudo-random number generator (PRNG) based on chaotic systems. In fact, designing a sequence of PRNG is utilized in several applications of cryptography such as; digital signatures, cryptosystems using keys and data hiding [38, 8]. The NIST tests are used to illustrate some randomness properties of the generated sequence from 3D-NCS, which after that adopted in the encryption algorithm. A new proposal are introduced to generate PRNG based on 3D-NCS. Four chaotic attractors are applied to generate PRNG are called NC(1), NC(2), NC(3) and NC(4), which turned out to have a high sensitivity and complexity in performance. Algorithm 2.2.1 shows the procedure to generate (PRNG).

**Algorithm 1: PRNS based on 3D-NCS**

**Input:** The initial values $(x_0, y_0, z_0) = (0, 0, 0)$, when $(a, b, c) = (100, 150, 100)$.
**Output:** Four PRNG, namely, NC(1), NC(2), NC(3) and NC(4), each of them with length 32-bits;

**For** $i = 1 : 3$ **do** Generate the chaotic sequences $X, Y$, and $Z$ from system (2).
Convert the floating number of $X, Y$, and $Z$ into 32-bit binary;
Shift 3-bits left rotation $X, Y$, and $Z$ sequences ;
Generate Sequences XY $= X \otimes Y$,
XZ $= X \otimes Z$, and YZ $= Y \otimes Z$;
Generate Sequence XYZ $= XY \otimes XZ \otimes YZ$;
Generate Sequence
XYZ = [XYZ XYZ], with length 64-bits;
**For** $j = 1 : 64$ do
NC($i$) = XYZ($j$);
**End**
**end**

Additionally, we used NIST-800-22 [30] to assure that the four sequences are random. NIST-800-22 contains 16 test of different statistical. The results of a statistical test are illustrated in Table 1. For the test, if the $p - value > 0.01$, then the generated sequence is passed, otherwise, the sequence is non-random. The initial values of the 3D-NSC of the test is to be $(x_0, y_0, z_0) = (0, 0, 0)$, with the parameters $(a, b, c) = (100, 150, 100)$.

*(b) Key schedule*

After generated PRNG, the key schedule values are acquired from the entries of PRNG, then these values are scrambled to generate a chaotic key schedule (CKS). We rearrange the entries of PRNG NC(1), NC(2), NC(3), and NC(4), in $B_k$ row, where $B_k = b_1, b_2, \cdots, b_{128}$, and $k = 1, \cdots, 32$ such that each row of table has $B_k$ = [NC(1), NC(2), NC(3), and NC(4)] with size 128- bits. Each element $b_i$ of $B_k$ essentially is corresponding a binary number of sequence. The final step is to choose 64-bits from each row Bk, through choosing the first bit, skipping the second, choosing the third, skipping the fourth, and so on in each series of the table. Algorithm 2.2.2 and Figure 7 shows the flowchart of the proposed key schedule.

*Table 1: The result of NIST statistical test of the sequences NC(1), NC(2), NC(3) and NC(4).*

| *NIST-test* | *NC(1)* | *NC(2)* | *NC(3)* | *NC(4)* | *Results* |
|---|---|---|---|---|---|
| *Frequency* | *0.8625* | *0.2032* | *0.7532* | *0.4251* | *Passed* |
| *Block-Frequency* | *0.1723* | *0.3720* | *0.7325* | *0.658* | *Passed* |
| *Cumulative-Sums* | *0.9873* | *0.9146* | *0.1032* | *0.3386* | *Passed* |
| *Runs* | *0.5715* | *0.7132* | *0.8319* | *0.7631* | *Passed* |
| *Longest-Run* | *0.5451* | *0.3251* | *0.6322* | *0.6791* | *Passed* |
| *Binary Matrix Rank* | *0.2017* | *0.6191* | *0.7613* | *0.8691* | *Passed* |
| *Discrete Fourier Transform* | *0.4211* | *0.0431* | *0.1198* | *0.1128* | *Passed* |
| *Non-Overlapping Templates* | *0.5353* | *0.4183* | *0.3386* | *0.3491* | *Passed* |
| *Overlapping, Templates* | *0.1658* | *0.8641* | *0.2297* | *0.2631* | *Passed* |
| *Maurers Universal Statistical* | *0.2414* | *0.1978* | *0.2157* | *0.2169* | *Passed* |
| *Approximate Entropy* | *0.1527* | *0.7387* | *0.7020* | *0.6121* | *Passed* |
| *Random-Excursions* | *0.9374* | *0.8551* | *0.8211* | *0.9232* | *Passed* |
| *Random-Excursions Variant* | *0.4167* | *0.4142* | *0.6422* | *0.7910* | *Passed* |
| *Serial Test-1* | *0.3122* | *0.04512* | *0.5357* | *0.6759* | *Passed* |
| *Serial Test-2* | *0.8122* | *0.6913* | *0.0769* | *0.723* | *Passed* |
| *Linear-Complexity* | *0.7523* | *0.2997* | *0.6652* | *0.3727* | *Passed* |

**Algorithm 1: Chaotic key schedule (CKS)**

**Input:** $B_k$ where $k = 1, \cdots, 34$;
**Output:** Key schedule, with size 34-rows and 64-bits;
**For** $k = 1 : 34$ **do**
**For** $j = 1 :$ step $2 : 128$ do
$\text{key}(k, j) = B_{k,j}$;
**End**
**end**

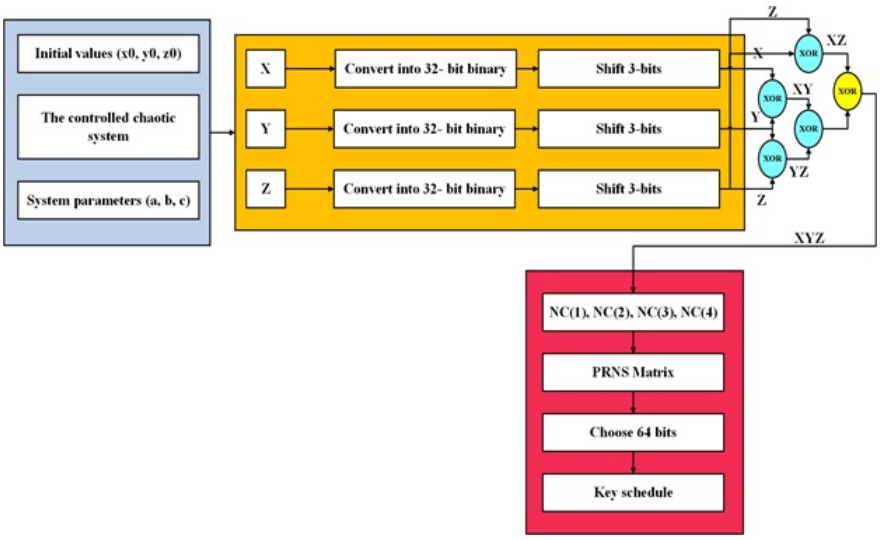


Figure 7: The flowchart of the proposed key schedule.

## 6. Chaotic Hight Algorithm

Encryption algorithms are divided into types or sets; The first type of these algorithms is called traditional algorithms which depended essentially on the blocks and its bitstream, such as; Encryption Standard (AES) [12], and Data Encryption Standard (DES) [32]. The other type is the modern algorithms such as; wavelet transform, chaotic systems, etc. Chaotic systems show high performance in encryption techniques [11]. In this section, we introduced an improved Hight algorithm with a new key schedule based essentially on system (2.2). After creating the (CKS) in the previous section, now is possible to hybridize the Hight algorithm with the (CKS). Figure 8 and algorithm 9 shows the procedure of the chaotic Hight algorithm (CHA).

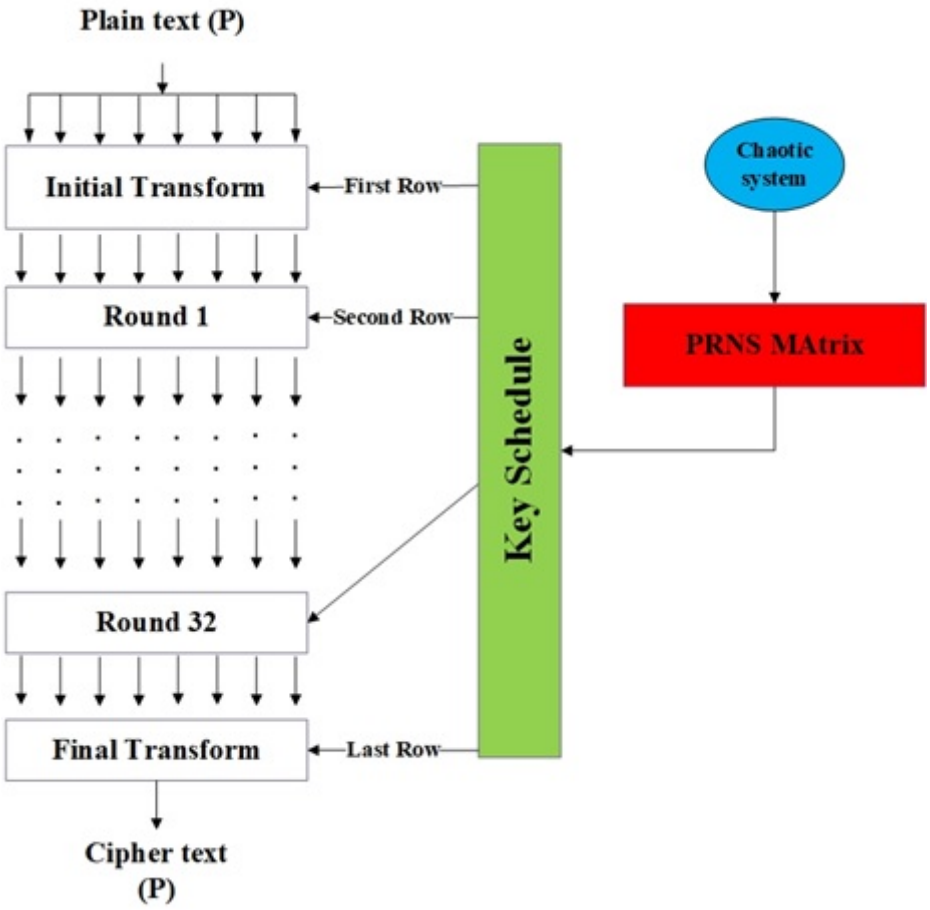


Figure 8: Chaotic Hight Algorithm.

**Algorithm 1: Chaotic Hight Algorithm (CHA)**

**Input:** Plaintext, key;
**Output:** Ciphertext;
**Initial Transformation** Palintext, key;
$X_{0,0} \leftarrow P_0 \otimes k_0$;
$X_{0,1} \leftarrow P_1$;
$X_{0,2} \leftarrow P_2 \otimes k_1$;
$X_{0,3} \leftarrow P_3$;
$X_{0,4} \leftarrow P_4 \otimes k_2$;
$X_{0,5} \leftarrow P_5$;
$X_{0,6} \leftarrow P_6 \otimes k_3$;
$X_{0,7} \leftarrow P_7$;
**Round transformation**
**For** i=1 to 32 **do**
$X_{i+1,1} \leftarrow X_{1,0}$;
$X_{i+1,3} \leftarrow X_{i,2}; X_{i+1,5} \leftarrow X_{i,4}$;
$X_{i+1,7} \leftarrow X_{i,6}$;
$X_{i+1,0} = X_{i,7} \otimes k_{4i+3}$ ;
$X_{i+1,2} = X_{i,1} \otimes k_{4i+2}$;
$X_{i+1,4} = X_{i,3} \otimes k_{4i+1}$ ;
$X_{i+1,6} = X_{i,5} \otimes k_{4i}$;
**Final transformation**
$C_0 \leftarrow X_{32,1} \otimes k_{38}$;
$C_1 \leftarrow X_{32,2}$;
$C_2 \leftarrow X_{32,3} \otimes k_{39}$;
$C_3 \leftarrow X_{32,4}$;
$C_4 \leftarrow X_{32,5} \otimes k_{40}$;
$C_5 \leftarrow X_{32,6}$;
$X_{0,6} \leftarrow X_{32,7} \otimes k_{41}$;
$C_7 \leftarrow X_{32,0}$;
**Ciphertext** $(C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7)$;

## 7. Cryptanalysis and Experimental Results

In this section, we introduced the cryptanalysis results of the proposed encryption system. In this simulation, we used a the dataset from the USC-SIPI image dataset with standard image processing. High ability to encrypted different types of images by transforming the pixels of images into random pixels difficult to recognize without any information about the plaintext images. The system of encryption for some images (color and grayscale images) are shown in Figure 10. Besides, Figure 11 and 12 illustrates plain (color and grayscale images) histograms, which have specific patterns, respectively.

http://sipi.usc.edu/database/
http://imageprocessingplace.com/root_files_V3/image_databases.htm

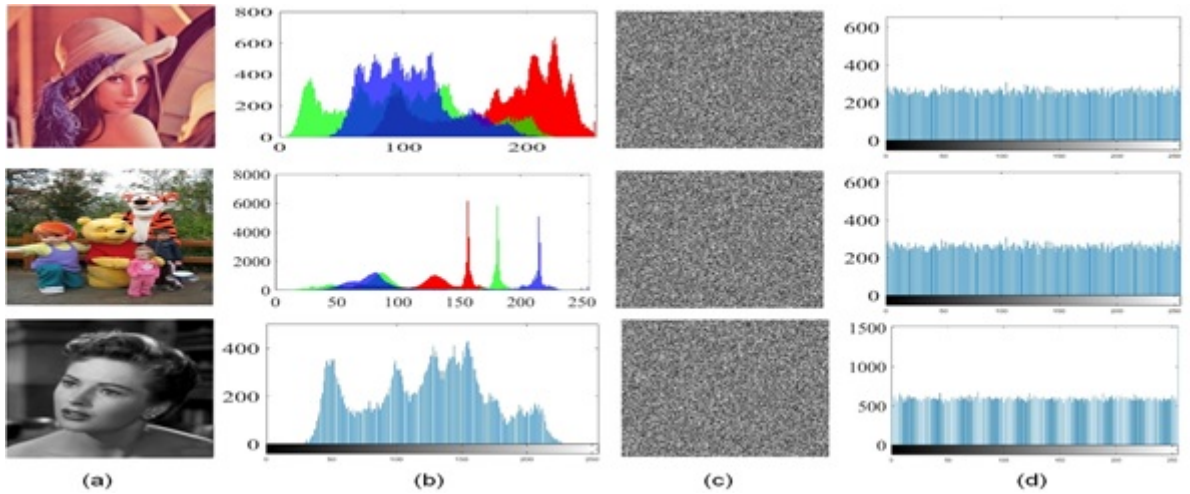


Figure 9: The results of simulation for the 3D-NCS: (a) Plain color and grayscale images; (b) the histogram of (a); (c) the cipher images of (a); and (d) the histogram of (c).

### *7.1. Histogram analysis*

The histogram measure represents the distribution of the image's pixel intensity values. Figures 11 and 12 illustrate the histogram of colour and grayscale images, respectively. They also show how the proposed encryption system achieve confusion property, where the original image is indiscernible.

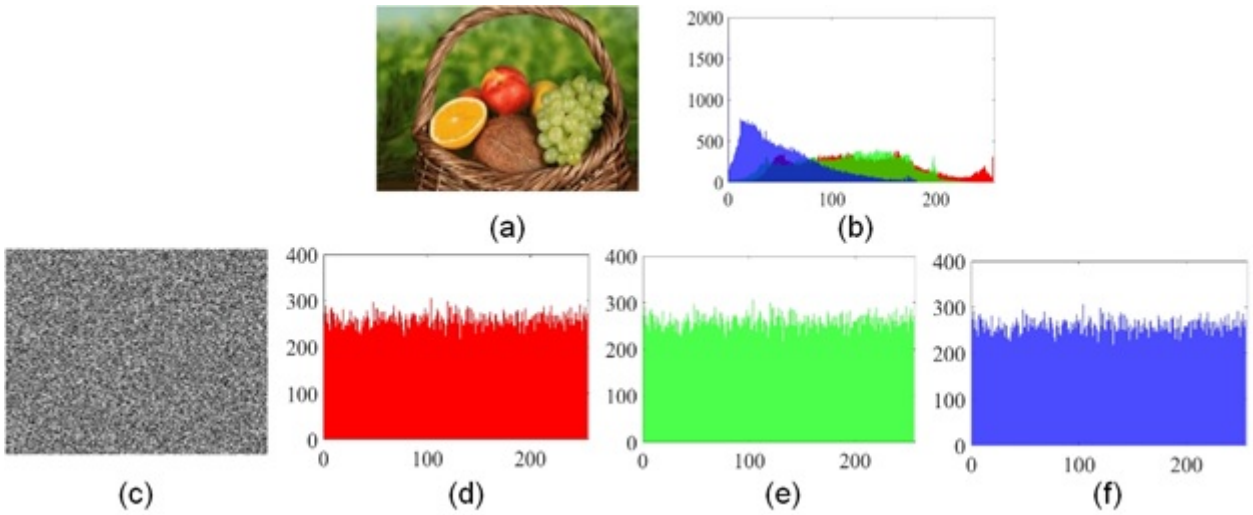


Figure 10: Histogram for the colour image: (a) plain image; (b) histogram of (a); (c) encryption of (a); (d)-(f) histograms of (c) red, green and blue components, respectively.

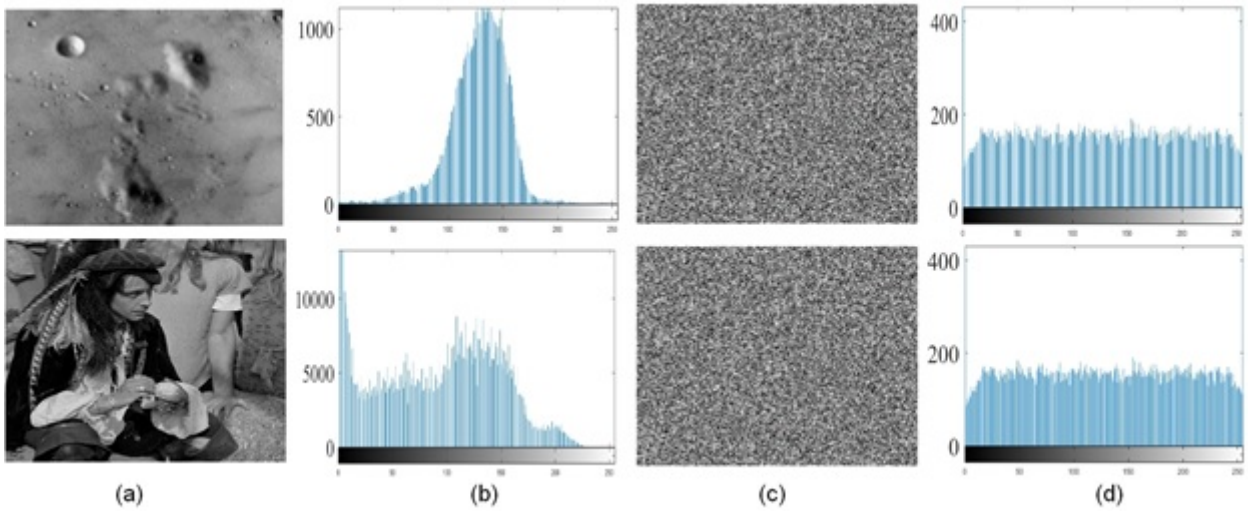


Figure 11: Distribution of the grayscale image pixel intensity values: (a) plain image; (b) histogram of (a); (c) encryption of (a); and (d) histogram of (c).

### *7.2. Correlation Analysis*

Correlation measure can be essentially defined as the relationship between two existing random variables. In image processing, it can be defined as the relation between two adjacent pixels in the image. Therefore, the encryption proposed is used to shatter the correlation between image adjacent pixels. Therefore, the correlation value after encryption refers to the efficiency of the encryption system. The results of the correlation of parrot images in three directions (horizontal, vertical, and diagonal) are shown in Figure 13. Table 2 illustrates the results of some previous work. The measure of correlation can be defined as follow:

$$\mathrm{CC} = \frac{E(x - E(x))E(y - E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \tag{7.1}$$

where

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad \textit{and} \qquad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

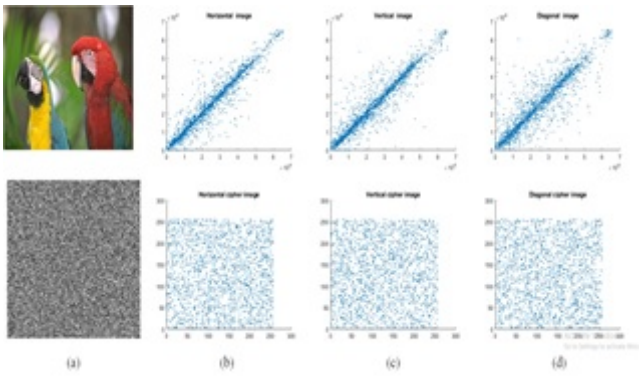

Figure 12: Correlation of pixels: (a) plain image and its cipher image, along with the (b) horizontal, (c) vertical, and (d) diagonal directions, respectively.

*Table 2: Correlation of several images.*

| Name | Original image | | | Cipher image | | |
|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| Lena | 0.960820 | 0.981383 | 0.947176 | -0.002032 | -0.012426 | -0.000198 |
| Female | 0.957683 | 0.983928 | 0.944619 | -0.002351 | -0.003171 | -0.000239 |
| Man | 0.986980 | 0.990941 | 0.975238 | -0.001038 | -0.002357 | -0.001534 |
| Tree | 0.963143 | 0.942524 | 0.925999 | -0.001129 | -0.003102 | -0.001762 |
| Moon | 0.902036 | 0.938978 | 0.903738 | -0.000113 | -0.001812 | -0.000723 |

### *7.3. Shannon entropy Shannon entropy*

Shannon C. in 1948, introduced a new measure of haphazardness to identifies the predicted information value in a message, it measures in bits units. This measure is named after its name (Shannon entropy), after that become one of the essential measures in information theory. In mathematics of Shannon entropy can be expressed as:

$$H(e) = \sum_{i=1}^{E} p(e_i) log \frac{1}{p(e_i)} \tag{7.2}$$

where $E$ is the total number of symbols $e_i$, and $p(e_i)$ denotes the probability of $e_i$. The entropy for Lena, Peppers, Tree and Couple images show in Table 3. Also, Table 4 illustrates the entropy of Lena image's with previous schemes.

*Table 3: Entropy for different images.*

| Image | Plain-image | Cipher image |
|---|---|---|
| Lena | 7.4429 | 7.9998 |
| Peppers | 6.5835 | 7.9997 |
| Tree | 7.5371 | 7.9989 |
| Couple | 6.2945 | 7.9998 |

*Table 4: The information entropy results.*

| Image name | Plain image | Cipher image | | | | |
|---|---|---|---|---|---|---|
| | | Our system | [33] | [? ] | [36] | [35] |
| Lena | 7.4429 | 7.9998 | 7.9977 | 7.9972 | 7.9972 | 7.9968 |

## 8. Conclusion

In this effort, a new 3D-hyperchaotic system is proposed with one equilibrium point, which we called 3D-NCS. Some performance measures of chaos are used to show the performance of 3D-NCS included phase diagram, LE, and Shanon entropy. Also, designed an electronic circuit for our chaotic system using the program proteus design suite. This system is then used to produce a pseudo-random number generator (PRNG), which is used to generate a key schedule for hight algorithm that realized confusion and diffusion. Our encryption system is used to encode multiple types of color and grayscale

images. Several analyzes evaluate the performance of our system through the use of many analytics such as; histogram, correlation pixels, and analyses of Shannon entropy. The proposed encryption system showed results of its analysis have high security and high efficiency compared with some other systems are highly performed. Besides, it has high efficiency and complexity compared to some other related works.

## References


[1] M. Alawida, J.S. Teh and A. Samsudin, *An image encryption scheme based on hybridizing digital chaos and finite state machine*, Signal Proces. 164 (2019) 249-266.

[2] D.S. Ali, N.A. Alwan and N.M. Al-Saidi, *Image encryption based on highly sensitive chaotic system*, AIP Conf. Proc. AIP Publishing, LLC. 2183(1) (2019) 080007.

[3] N. M. Al-Saidi, MG. Nadia, S. S. Al-Bundi and J. N. Al-Jawari, *A hybrid of fractal image coding and fractal dimension for an efficient retrieval method*, Comput. Appl. Math. 37(2) (2018) 996–1011.

[4] N.M. Al-Saidi and A.H. Ali, *Towards enhancing of fractal image compression performance via block complexity*, Ann. Conf. New Trends Inf. Commun. Technol. Appl. IEEE (2017) 246–251.

[5] N. M. Al-Saidi, M. R. M. Said and W. A. M. Othman, *Password authentication based on fractal coding scheme*, Journal of Applied Mathematics, 2012 (2012).

[6] N.A. Alwan, A.Y. Yousif and N.M. Al-Saidi, *Performance-enhancing of RSA public key via three-dimensional hyperchaotic system*, AIP Conf. Proc. 2325(1) (2021) 020027.

[7] A.M. Asl, A. Broumandnia and S.J. Mirabedini, *Scale invariant digital color image encryption using a 3D modular chaotic map*, IEEE Access 9 (2021) 102433–102449.

[8] M. Şahin Açikkapi, F. Özkaynak and A. Bedri Özer *Side-channel analysis of chaos-based substitution box structures*, IEEE Access 7 (2019) 79030–79043.

[9] C. Cao, K. Sun and W. Liu, *A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map*, Signal Proces. 143 (2018) 122–133.

[10] H. Diab and A.M. El-Semary, *Secure image cryptosystem with unique key streams via hyper-chaotic system*, Signal Proces. 142 (2018) 53–68.

[11] A.K. Farhan, N.M.G. Al-Saidi, A.T. Maolood, F. Nazarimehr and I. Hussain, *Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder*, Entropy 21(10) (2019) 958.

[12] S. Heron, *Advanced encryption standard (AES)*, Network Security 2009(12) (2009) 8–12.

[13] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.S. Koo and S. Chee, *HIGHT: A new block cipher suitable for low-resource device*, In International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg, (2006) 46-59.

[14] Z. Hua and Y. Zhou, *Image encryption using 2D Logistic-adjusted-Sine map*, Inf. Sci. (Ny) 339 (2016) 237–253.

[15] Z. Hua, Y. Zhou, C.M. Pun and C.P. Chen, *2D Sine Logistic modulation map for image encryption*, Inf. Sci. (Ny) 297 (2015) 80–94.

[16] Z. Hua,F. Jin, B. Xu and H. Huang, *2D logistic-sine-coupling map for image encryption*, Signal Proces. 149 (2018) 148–161.

[17] M. Khan and F. Masood, *A novel chaotic image encryption technique based on multiple discrete dynamical maps*, Multimedia Tools Appl. 78(18) (2019) 26203–26222.

[18] L.R. Knudsen, *Practically secure Feistel ciphers*, Int. Workshop on Fast Software Encryption, Springer, (1993) 211–221.

[19] S. Koppu and V.M. Viswanatham, *A fast enhanced secure image chaotic cryptosystem based on hybrid chaotic magic transform*, Model. Simul. Eng. 2017 (2017) Article ID 7470204.

[20] W. Liu, K. Sun and C. Zhu, *A fast image encryption algorithm based on chaotic map*, Optics Lasers Engin. 84 (2016) 26–36.

[21] H. Liu and X. Wang, *Color image encryption based on one-time keys and robust chaotic maps*, Comput. Math. Appl. 59(10) (2010) 3320–3327.

[22] E.N. Lorenz, *Deterministic nonperiodic flow*, J. Atmospheric Sci. 20(2) (1963) 130–141.

[23] G. Maddodi, A. Awad, D. Awad, M. Awad and B. Lee, *A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding*, Multimed. Tools Appl. 77(19) (2018) 24701–24725.

[24] G. Makris and I. Antoniou,*Cryptography with chaos*, Proc. 5th Chaotic Model. Simul. Int. Conf. Athens, Greece, (2012) 12–15.

[25] A. Nag, J. Singh, S. Khan, S. Ghosh, S. Biswas, D. Sarkar, and P.P. Sarkar, *Image encryption using affine transform and XOR operation*, Int. Conf. Signal Proces. Commun. Comput. Network. Technol. (2011) 309–312.

[26] H. Natiq, M.R.M. Said, N.M. Al-Saidi and A. Kilicman, *Dynamics and complexity of a new 4d chaotic laser system*, Entropy 21(1) (2019) 34.
[27] H. Natiq, N.M. Al-Saidi and M.R.M. Said, *Complexity and dynamic characteristics of a new discrete-time hyperchaotic model*, Second Al-Sadiq Int. Conf. Multidiscip. IT Commun. Sci. Appl. (2017) 1–6.
[28] H. Natiq, N.M.G. Al-Saidi, M.R.M. Said and A. Kilicman, *A new hyperchaotic map and its application for image encryption*, Eur. Phys. J. Plus, 133(1) (2018) 6.
[29] H. Poincare, *Science et Methode*, Flammarion, Paris, 1908.
[30] A. Rukhin, J. Soto, J. Nechvatal, M. Smid and E. Barker, S.D. Leigh, M. Levenson, M. Vangel, D.L. Banks, N.A. Heckert, J.F. Dray Jr. and S.C. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Pub Series, 2021.
[31] C.E. Shannon, *Communication theory of secrecy systems*, Bell Syst. Technical J. 28(4) (1994) 656–715.
[32] *Standard, Data Encryption and others*, Federal information processing standards publication 46, National Bureau of Standards, US Department of Commerce 23 (1977).
[33] M. T. Wazi,D. S. Ali,N. M. Al-Saidi and N. A. Alawn, *A secure image cryptosystem via multiple chaotic maps*, Discrete Math Algorithms Appl. 2021 (2021) 2150141.
[34] X. Wu, D. Wang, J. Kurths and H. Kan, *A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system*, Inf. Sci. (Ny). 349-350 (2016) 137–153.
[35] Y. Wu,J. P. Noonan and S. Agaian, *NPCR and UACI randomness tests for image encryption*, J. Selected Areas Telecommun. 1(2) (2011) 31–38.
[36] L. Xu, X. Gou, Z. Li and J. Li, *A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion*, Optics Lasers Engin. 91 (2017) 41–52.
[37] W. Yan, Z. Jiang, X. Huang and Q. Ding, *A Three-Dimensional Infinite Collapse Map with Image Encryption*, Entropy 23(9) (2021) 1221.
[38] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu and J. Liu, *A novel block encryption algorithm based on chaotic S-box for wireless sensor network*, IEEE Access 7 (2019) 53079–53090.
[39] D. Younus, N.M. Al-Saidi and W.K. Hamoudi, *Secure optical communication based on new 2D-hyperchaotic map*, AIP Conf. Proc. AIP Publishing LLC. 2183(1) (2019) 090006.
[40] Y. Zhang, L. Zhang, J. Zhou, L. Liu, F. Chen and X. He, *A review of compressive sensing in information security field*, IEEE Access 4 (2016) 2507–2519.