INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

WAM 3D Discrete Chaotic Map for Secure Communication Applications

Ali Akram Abdul-Kareem
Iraqi Commission for Computers and Informatics
Information Institute for Postgraduate Studies
Baghdad, Iraq

Waleed Ameen Mahmoud Al-Jawher
Uruk University
Baghdad, Iraq
Email: phd202020559@iips.icci.edu.iq

Submitted: 30/11/2022. Revised edition: 31/3/2023. Accepted: 31/3/2023. Published online:
DOI: https://doi.org/10.11113/ijic.v13n1-2.419

***Abstract*—Chaotic systems have become widely adopted as an effective way for secure data communications, because of its simple mathematical complexity and good security. The relationship between encryption algorithms and chaos systems has gained a lot of attention in the past few years, since it avoids the data spreading as well as lower the transmission delay and costs. In this paper a novel 3D discrete chaotic map is proposed for data encryption and secure communication and named as WAM. For secure communication, the Pecora and Carroll (P-C) method was utilized to achieve synchronization between the master system and the slave system. The simulation results of WAM 3D discrete chaotic map showed that the system has a chaotic behavior and a characteristic randomness and can pass 0-1, Lyapunov exponent (LE) and NIST tests which are usually used to check chaotic behavior. The statistical outcomes of the LE test were 0.0193, the frequency test (FT) was 0.4237, and the run test (RT) yielded a value of 0.0607. As a result, it enrich the theoretical basis of the equations and implementation of chaos, and it is superior for encryption algorithms and communication security applications.**

***Keywords*—Chaotic map, secure communication, WAM 3D discrete, NIST, LE**

I. INTRODUCTION

Over the past few years, numerous studies have been put for chaos being a ubiquitous natural phenomenon. In fact, chaotic features offer many advantages when used in the field of artificial intelligence, economics, signals processing, secure communications, and so on [1-3]. In particular, chaotic systems are frequently applied in secure communications because they can generate complex, non-linear, initial condition sensitive, and low computational complexity chaotic currents [4-7]. For secure communication to take place, the first step is to encrypt the data to be delivered. Then the encrypted data is transmitted from the sender to the receiver over an open public channel where the transmitted data is likely to suffer from theft attacks. Once the encrypted data is stolen, it is difficult for the attacker to recover the original data due to the random nature of the chaotic systems [8-12]. In addition, the process of synchronizing chaotic systems is one of the important factors for achieving secure communication [11]. Although it is difficult to synchronize chaotic systems dynamically, the Pecora and Carroll (P-C) demonstrated in the 1990s that chaotic systems can be synchronized using different initial conditions. Chaos synchronization requires two specific systems: a primary system and a subsystem. These two systems are characterized using conventional equations and available parameter, noting that the main system leads the subsystem. Thus, secure communication based on chaotic systems can be achieved [14-18]. This research presents a novel three-dimensional chaotic system for data encryption and secure communication. The Pecora and Carroll (P-C) method was utilized to synchronize two chaotic systems in order to secure the transmission between the transmitter and receiver. In addition to employing NIST tests to evaluate the system's performance, the proposed system will also be subjected to randomness performance evaluations.

The rest of this research is arranged in the following manner. The second section contains related works. Section three gives a historical review of the most common chaotic systems is presented. Section four gives the detail description for the proposed 3D discrete chaotic map. Section 5, presents a comparison to generate stream ciphers and presents the results of several tests that carried on the proposed chaotic system. Section 6, presents the synchronization performance of the proposed chaotic system verified by nonlinear control laws. Finally, the proposed system is implemented in the image encryption algorithm to confirm its effectiveness.

II. Related Work

Due to the simplicity of generating chaotic strings with broad ranges and low computational complexity, chaotic maps are preferred over traditional roads for securing communications. Although all chaotic maps are sensitive to initial conditions and can generate long chains, the number of map dimensions determines the sensitivity and length of each map. Increasing the dimensions of chaotic maps, however, increases their execution time, limiting their use in real-time security applications. Here are examples of suggested chaotic maps for addressing these issues: Pisarchik, A *et al*. [3] proposed a hybrid communication system consisting of two identical oscillators of six orders, equally chosen between the transmitter and the receiver, each exhibiting synchronization to a huge number of chaotic attractors. Zolfaghari-Nejad, M *et al*. [19] presented a new, non-Shilnikov chaotic system with a two zeros of eigenvalues positioned on the axis with a single equilibrium point and three eigenvalues at the origin. Simulation analysis of the system reveals applicability of the chaotic system in real applications. Abdullah, H. A. *et al*. [20] suggested a hybrid chaotic system partially combined from Rössler and Henon. Randomization and synchronization performance were statistically verified and experiments proved that it can be used to develop functional synchronization and encryption algorithms for secure communications applications for images, video, and voice. J. Wen *et al*. [1] introduced a five-dimensional chaotic system with a hidden attractor. Although it corresponds to the class of unbalanced chaotic systems with hidden attractor, this system can easily create hidden chaotic attractors whose static conditions can be very large. They concluded that the system has a complex dynamic behavior that makes it suitable for secure communication and image encryption. Dong, C [21] presented a new independent chaotic system with two stable nodefoci which can produce two wings embedded chaotic attractors. Dynamic analysis tests showed that the proposed chaotic system has rich dynamics, which has some interesting properties of the parameters, initial conditions and chaotic behavior. The strength of the findings in the above systems motivates us to go down the same path. In this study, a novel chaotic system is presented for secure data communication. The randomness performance of the proposed system was examined using 0-1 tests, Lyapunov exponents and phase portraits.

III. Historical review

Chaos techniques have become very popular over the past few years. Interestingly, some such as the Logistic, Lorenz, Henon and Rossler map are well known not only among computer scientists but also among economists, physicists and engineers. In addition to the huge number of theoretical studies, the simplicity of the equations and flexibility of application and low computational complexity encouraged scientists to apply these chaos techniques in various fields of study [22-24]. These properties allow computer scientists to simulate different chaotic phenomena, suggest new chaotic methods, or hybridize two or more chaotic maps, or improve existing chaotic methods, or synchronize two or more chaotic systems. Chaos techniques can be classified into two main categories: continuous and discrete maps. Discrete maps are usually based on the discrete time parameter, and the most common map in this branch is the logistics map. John von Neumann suggested using this map as a random number generator in the late 1947. The mathematical description for the logistic map is given by [25]:

$$X(n+1) = a\,x(n) - b\,x(n)2 \quad (1)$$

Edward Lorenz was able in 1963 to arrive at three differential equations now known as Lorenz's equations. These three equations represent the chaotic Lorenz system, as shown below [26].

$$dx/dt = SIGMA\,(y - x) \quad (2)$$
$$dy/dt = RHO\,x - y - x\,z \quad (3)$$
$$dz/dt = x\,y - BETA\,z \quad (4)$$

In 1976, the mathematician and astronomer Michel Henon proposed the Henon map, which is a discrete-time dynamical system. Henon map form can be described using the following expression [27]:

$$x(n+1) = 1 - ax(n)2 + y(n) \quad (5)$$
$$y(n+1) = bx(n) \quad (6)$$

In the same year, German biochemist Otto Rössler proposed a continuous dynamic system of three nonlinear differential equations. This system exhibits dynamics associated with chaotic properties. The equation describing this map is given below [28]:

$$dx = -y - z \quad (7)$$
$$dy = x + ay \quad (8)$$
$$dz = b + z(x-c) \quad (9)$$

Whether the chaotic system is based on discrete or continuous time parameters, the multidimensional system has stronger randomness, more chaotic attractors, better confidentiality, larger secret key space, and higher efficiency in securing communications and data [29]. In this article, a multidimensional discrete chaotic system is proposed to be used in constructing chaotic sequence and chaotic encryption. In the next sections, the details of the proposed chaotic system will be discussed and its performance analysis.

IV. The Proposed 3D discrete chaotic map (WAM)

Low-dimensional chaotic maps are easy to implement due to their simple structure, but they often suffer from dynamic degradation radically different from theoretical expectations. Therefore, the original idea presented by this paper is to propose a new 3D discrete chaotic map, using new sets of nonlinear equations, and named as WAM and described by the following equations:

$$Xn+1 = 1 - a\,Xn\,Yn - Xn2 - Yn2 - b \sin(Zn2) \quad (10)$$
$$Yn+1 = Xn \quad (11)$$
$$Zn+1 = \pi - Yn - c \sin(Zn) \quad (12)$$

Note that a, b, and c are the parameters of system control while x, y, and z are system variables. The addition of the trigonometric functions and the nonlinear terms of the above equations increased the randomness of the proposed WAM 3D discrete chaotic map. In addition, the proposed chaotic system contains four nonlinear terms (xy, x2, y2, z2), where by the first equation notably contains four cross-product terms, and the first and third equations contain a sine function, so it is definitely suitable for encryption and communication security applications. Through a series of MATLAB simulation and modeling which is given in Fig. 1, the 3D projections of the phase portraits of the proposed system were obtained used the following values for the control parameters: a = 1.52, b = 0.05 and c = 0.05 and the initial values used are: X (0) = 0.3, Y (0) = 0.2 and Z (0) = 0.1 as shown in Fig. 2. It is clear that the attractors have a peculiar shape that indicates that the proposed method will have a strong chaotic behavior, and contains several new dynamic characteristics.

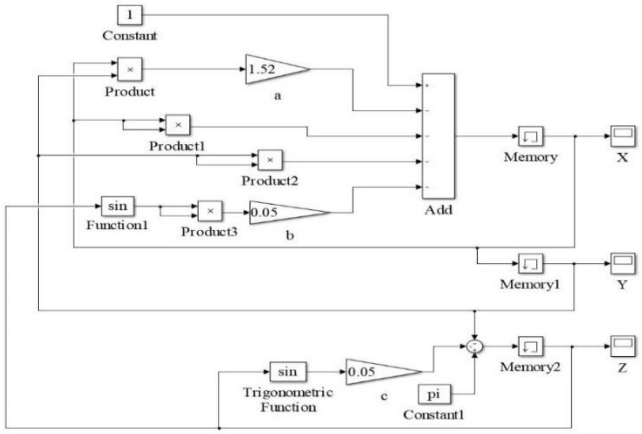

Fig. 1. MATLAB-Simulink model of 3D discrete chaotic map

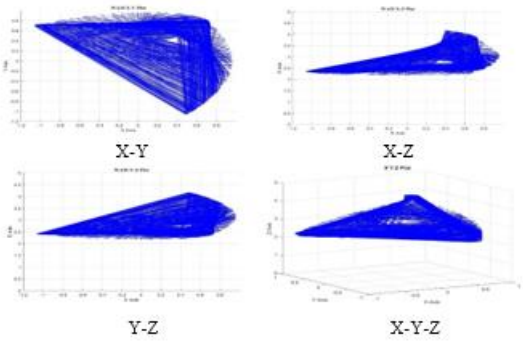

Fig. 2. The 3D discrete chaotic map phase portraits

V. Experimental Analysis

Several statistical analysis tests were carried on the proposed 3D discrete chaotic map in order to confirm its strong behavior. Fig. 3 provides an overview of the dynamics of the proposed 3D discrete chaotic map. It is clear from this from figure for the signal amplitude against time, the probability distribution for all values is constant, which means that the probability of producing any random number remains the same under the dynamics of the proposed system. This preliminary result proves the randomness of the chaotic behavior of the proposed 3D discrete chaotic map.

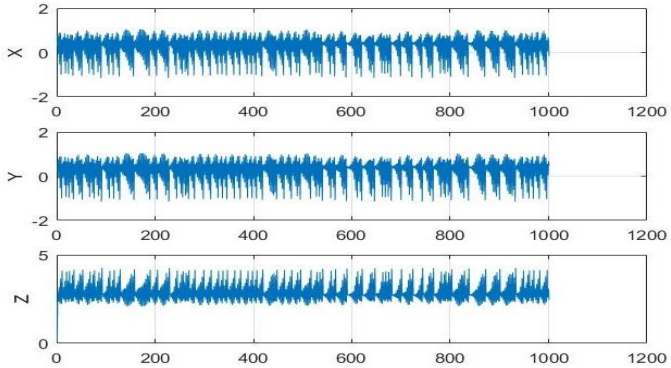

Fig. 3. Waveforms of 3D discrete chaotic map

A. Chaotic Behavior of The Proposed 3D discrete chaotic map

The Lyapunov exponent (LE) test was used to check the chaotic behavior of the system. The Lyapunov exponent test for chaotic systems are values used to determine whether or not a system behaves in a chaotic manner. For a chaotic system, at least one value must be a positive number, and the system is periodic when LE is negative. Moreover, when LE is 0, this indicates that bifurcation has occurred. The Jacobian matrix was used during the application of Lyapunov exponent test [30, 31]:

$$J = \begin{matrix} -2x - ay & -2y - ax & -2bzcos(z\text{^}2) \\ 1 & 0 & 0 \\ 0 & -1 & -c\,cos(z) \end{matrix} \quad (13)$$

The result obtained from the above equation were: LE1 = 0.0193, LE2 = -0.022 and LE3 = -0.1917, and Lyapunov dimension is 1.8778. The positive value in this test proves that the proposed 3D discrete chaotic map has chaotic properties. Fig. 4 shows each calculated exponent.

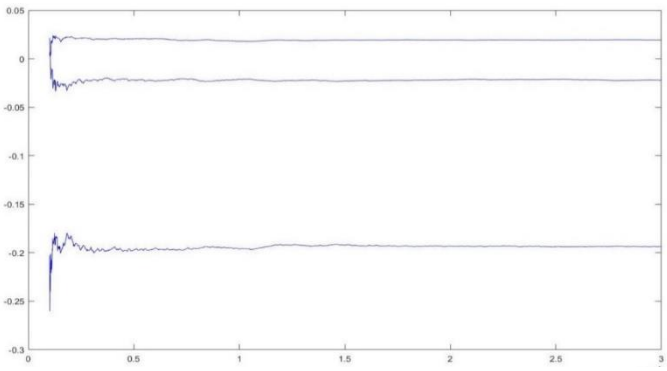

Fig. 4. . Lyapunov exponents (LE) of 3D discrete chaotic map

B. Zero-One Test

The zero-one test was introduced by Gottwald and Melbourne in [32] and developed in [33] to distinguish

between periodic and chaotic behavior in dynamical systems. The procedure followed in the 0-1 test are**:**

- Assume the test input is D(n) which is a one-dimensional time series of n = 1, 2, 3....N.
- Define R where as a real number and greater than zero.
- Calculate the translation variables p(n+1) and q(n+1) by:

$$p(n+1) = p(n) + D(n)\cos(nR) \quad (14)$$

$$q(n+1) = q(n) + D(n)\sin(nR) \quad (15)$$

- Apply the mean square displacement (MSD) using the following equation:

$$MSD\ (n) = \lim_{n\to\infty} \frac{1}{N} \sum_{j=1}^{N} ([p(j+n) - p(j)]^2 + [q(j+n) - q(j)]^2) \quad (16)$$

- Finally, obtain the approximation growth average (K) using the following equation:

$$K = \lim_{n\to\infty} \frac{\log MSD\ (n)}{\log n} \quad (17)$$

To prove that the system has chaotic properties, the value of K must be close to 1. In contrast, by selecting the value of K as 0, this indicates a non-chaotic system [31-35]. Values of K that are obtained for the variables of the proposed system given as: Kx = 0.9958, Ky = 0.9952, and Kz = 0.9948. These results prove the chaotic properties of the proposed 3D discrete chaotic map as its clear nearly to 1.

C. Autocorrelation function

The autocorrelation function of multidimensional chaotic dynamics is one of the main tools for measuring the randomness property of chaotic systems by measuring the self-similarity of the signal across different delay times [5]. The quasi-flat autocorrelation function shown in Fig. 5 proved the randomness properties of the sequences generated by the proposed 3D discrete chaotic map and thus difficult to exploit via correlation attacks.

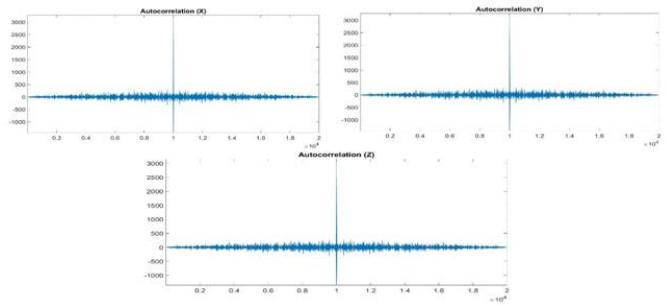

Fig. 5. Autocorrelation function for each component of the proposed 3D discrete chaotic map, (a) x component, (b) y component, (c) z component

D. The Random Binary Numbers Generator

In the context of the relationship between chaos and security technologies, one of the stages of encryption needs to generate independent random binary streams by separate chaotic dynamic systems [20, 34]. In this section, independent stochastic binary currents are generated based on matching two chaotic systems operating at the same time, with the same control parameters but with different initial conditions. The values of the parameters used are (a=1.52, b= 0.05 and c= 0.05) and initial values used for systems (X1=0.3 Y1=0.2, Z1=0.1, X2 = 0.2, Y2 = 0.1, and Z2 = 0.2). Chaotic systems were matched according to equations (18-20) as shown in Fig. 6.

$$BX=\begin{cases}1, & if\ \ X2 < X1\\ 0, & if\ \ X2 \geq X1\end{cases} \text{ where X1 (0)} \neq \text{X2 (0)} \quad (18)$$

$$BY=\begin{cases}1, & if\ \ Y2 < Y1\\ 0, & if\ \ Y2 \geq Y1\end{cases} \text{ where Y1 (0)} \neq \text{Y2 (0)} \quad (19)$$

$$BZ=\begin{cases}1, & if\ \ Z2 < Z1\\ 0, & if\ \ Z2 \geq Z1\end{cases} \text{ where Z1 (0)} \neq \text{Z2 (0)} \quad (20)$$

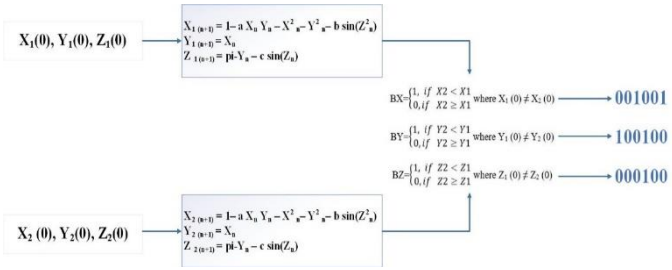

Fig. 6. Random Binary Numbers Generator

E. The Randomness Tests

A set of tests has been adopted to test the stochastic properties of long binary sequences produced by chaotic systems [35]. It has been proven that the sequence of zeros and ones is completely random for the series of binary numbers generated using proposed system by accepting the null hypothesis. In addition, the statistical test results listed in Table I are very encouraging and show that the proposed 3D discrete chaotic map has optimal encryption properties and thus can be exploited to design new stream ciphers.

TABLE I. THE RANDOMNESS TESTS

The Randomness Tests	BX	BY	BZ	Evaluation
Frequency (MonoBit) test	0.4237	0.5485	0.8415	Passed
Frequency (block = 1000) test	0.4812	0.4812	0.4812	Passed
Run test	0.0607	0.0410	0.0711	Passed
Longest run of ones	0.2376	0.0347	0.0163	Passed
Binary matrix rank test	0.1575	0.1575	0.0372	Passed
Discrete Fourier Transform (DFT) test	0.0203	0.0203	0.0422	Passed
Maurer test	0.8815	0.8771	0.8692	Passed
Approximate entropy test	0.5224	0.5228	0.5123	Passed
Cumulative sum test – Forward	0.8148	0.9586	0.9908	Passed
Cumulative sum test – Reverse	0.6292	0.7224	0.8973	Passed
Non Overlapping Test	0.8919	0.8919	0.8919	Passed

VI. SYNCHRONIZATION OF 3D DISCRETE CHAOTIC MAP

Achieving synchronize chaotic system was a difficult task. Usually, the intrinsic properties of chaotic systems resist

synchronization. In 1990s of the last century, both Pecora and Carroll (P-C) abled to implement chaotic systems synchronization by starting with different initial conditions [14-18, 36]. In this section, the synchronization of 3D discrete chaotic map is studied and verified using (P-C) method and applied for a secure communication. The synchronization block diagram of the proposed 3D discrete chaotic map are shown in Fig. 7.

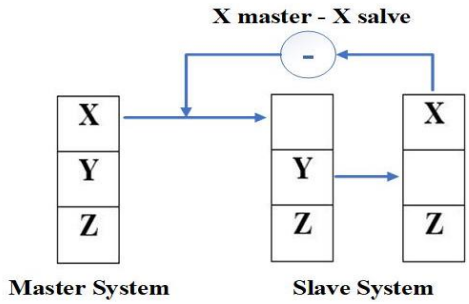

Fig. 7. The block diagram of 3D discrete chaotic map based on P-C Synchronization

Equations (10-12) gives the primary system equations of the proposed 3D discrete chaotic map synchronization, in contrast, Y-secondary and Z-secondary can be formulated in first-order secondary subsystem as given in Equations (21) and (22).

$$Yn+1 = Xn \quad (21)$$

$$Zn+1 = pi - Yn - c \sin(Zn) \quad (22)$$

While X and Z can be formulated in the second order of the secondary system as mentioned in equations (23) and (24).

$$Xn+1 = 1 - a\,Xn\,Yn - Xn2 - Yn2 - b \sin(Zn2) \quad (23)$$

$$Zn+1 = pi - Yn - c \sin(Zn) \quad (24)$$

The initial values of the primary system that used in equations (10-12) are (X0, Y0, Z0) = (0.3, 0.2, 0.1). While the initial values of the secondary system that used in equations (21-24) are (X0, Y0, Z0) = (-0.1, 0.3, -0.2), respectively with control parameters values (a, b and c) defined as (1.52, 0.05, 0.05), respectively. The synchronization was implemented between X-primary and X- secondary. Fig. 8 shows the pre-synchronization behavior of X-primary and X-secondary, which shows high randomness and very high error rate.

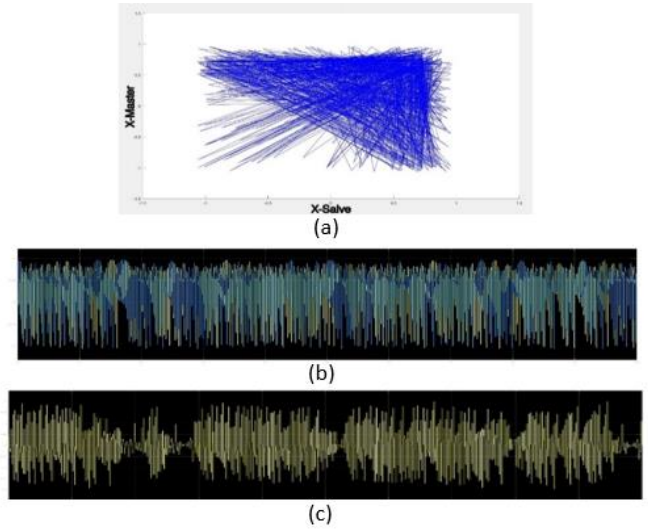

Fig. 8. Pre-synchronization behavior: (a) phase portraits of X primary, X secondary, (b) X primary and X secondary, (c) error rate (e = error signal)

Once the simulation is started with the above values, the behavior of the X variable of the primary system is obtained along with the signal of the X variable of the secondary system and these signals change according to each other as shown in Fig. 9. These signals synchronize and the error signal equals zero in a very short time, which is conclusive evidence of the high sensitivity of the proposed system as shown in Fig. 9c.

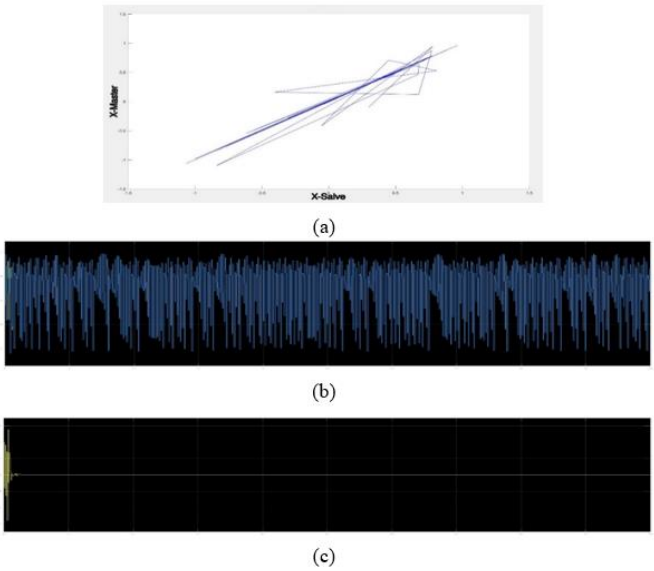

Fig. 9. Post-synchronization behavior (a) phase portraits of X primary, X secondary, (b) X primary and X secondary, (c) error rate (e = error signal)

VII. Data Security Simulation

To confirm the effectiveness of the proposed chaotic system, the chaotic system is tested by generating an encryption key in an image encryption system. The 3D discrete chaotic map initial conditions and control parameters that used are X(1) = 0.3, Y(1) = 0.2, Z(1) = 0.1, a = 1.52, b = 0.05, c = 0.05.

VIII. Image Encryption Using The Proposed 3D discrete chaotic map

The various characteristics of proposed system are explored using several 512×512 color images, namely: Lena, pepper, tree, baboon, Barbara, bird, camel, flowers and satellite image. The following procedure are followed in the encryption system.

- Separate the color image into 3 primary channels (red, green, and blue).
- Convert the red, green, and blue channels into 1D vectors VR, VG, and VB.
- Generating an encryption key from the 3D discrete chaotic map based on equations (10-12).
- The pixel positions in each channel are confused based on the 3D encryption key (X, Y and Z) obtained from the 3D discrete chaotic map.
- Convert the 3D encryption key (X, Y and Z) into its binary representation (BX, BY, and BZ) based on Equations (18-20).
- The binary 3D encryption key is converted in to their decimal representations.
- The pixel values of confused channels are diffused by XOR computation with (BX, BY and BZ).

The main block diagram of the above procedure is given in Fig. 10.

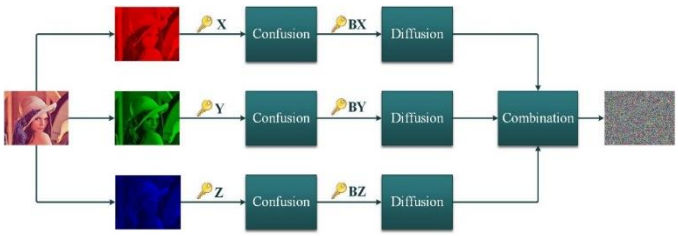

Fig. 10. Shows the main block diagram of the proposed method

IX. Statistical Evaluation of The Novel Encryption System

The encryption algorithms can be cracked using statistical analysis attacks. Therefore, histogram analysis and correlation coefficient are used to study the pixel distribution of the encrypted image to verify the efficiency of the proposed method against statistical attacks.

A. The Histogram

The Histogram is one of the most statistical tests that reveal the distribution of pixel values of an image. The histogram of the plain image is fundamentally different from the histogram of the encrypted image. Usually, the histogram of a plain image has different peaks. In contrast, the histogram of the encrypted image is uniform. Therefore, the color distribution information remains unknown to the attackers [37-42]. Fig. 14 shows the histogram of red, green and blue channels of the plain and encrypted images using the proposed method, which showed an effective result.

B. Correlation Coefficient

The pixel in the original image is strongly correlated to neighboring pixels from all directions. Therefore, the correlation coefficient is used to express this statistical relationship. In meaningful images the value of the correlation coefficient is close to 1. In contrast, the value of the correlation coefficient is close to 0, in encrypted images. Therefore, one of the most important objectives of effective encryption algorithms is to obtain an encrypted image with the lowest possible correlation [43-46]. Fig. 11 shows the close statistical relationship between the pixels in the original image in all directions, where all the pixels are close to each other. In contrast, Fig. 12 shows the random distribution of pixels in the encrypted image produced by the proposed method.

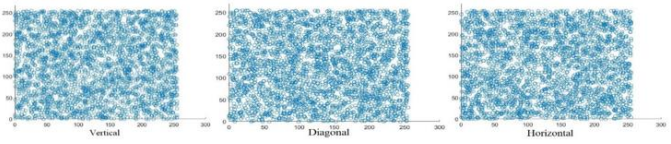

Fig. 11. Correlation coefficient of 3000 random pixels in the vertical, horizontal, and diagonal directions of the bird image

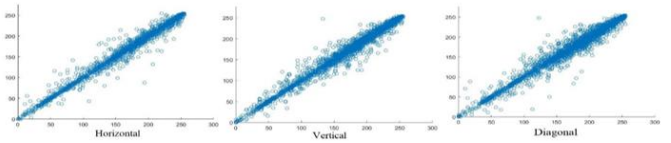

Fig. 12. Correlation coefficient of 3000 random pixels in vertical, horizontal, and diagonal directions for ciphered bird image

C. Analysis of Information Entropy

The Entropy is an analytical measure of the randomness level in a cryptographic system. Shannon [47] proposed the following mathematical equation to calculate the entropy:

$$IE(S)= - \Sigma \text{▒} [P(S)\times [Log]_2 P(S)] \quad (25)$$

where P(S) indicates the probability of S symbol appearing. It is noteworthy that pixel values can be represented by 8-bit binary data with 256 color levels. Therefore, the maximum value of the entropy is 8, which means that all levels of color in the encrypted image have an equal probability of appearing [37, 39, 48-51]. The entropy of the red, green, and blue channels of the encrypted images is shown in Table II, indicating that the average entropy value is close to 8, which means that the encrypted images have sufficient randomness. Table III shows the outstanding performance and competitive results of the 3D discrete chaotic map compared to other chaotic systems.

D. Analysis of The Differential Attack

It is clear that the attackers seek to find a relationship between the normal image and the encrypted image by making some possible changes to the normal image and then encrypting the image before changing and after changing. Metrics such as NPCR and UACI were used to estimate resistance to differential attack and to analyze the effect of a small change in the encoded

image [37, 44, 52-55]. The results in Table IV show that the proposed algorithm has a superior performance compared to the other methods.

E. Key Sensitivity Analysis

It is expected for the proposed chaotic system to be very sensitive to the initial conditions, a very small change in the initial conditions will lead to a large change in the output. Since the proposed image encryption algorithm uses a discrete chaotic map that is very sensitive to any change in initial conditions. To prove the sensitivity of the proposed 3D discrete chaotic map, simple changes were made to the initial conditions of the matched key in the decryption process. The original image is first encrypted with: X(1) = 0.3, Y(1) = 0.2, Z(1) = 0.1, a = 1.52, b = 0.05, c = 0.05. Then, the image is decrypted using the same conditions except the initial condition value (a) is changed slightly to 1.520000000001. Fig. 13 displays Lina's color image and peppers' color image as a test images. It is clear, the decryption process with slightly different initial conditions fails completely. Thus, the secret key generated using the proposed chaotic system is very sensitive. It is clear from the figure, that the encrypted images obtained from the proposed algorithm are robust against brute force attacks.

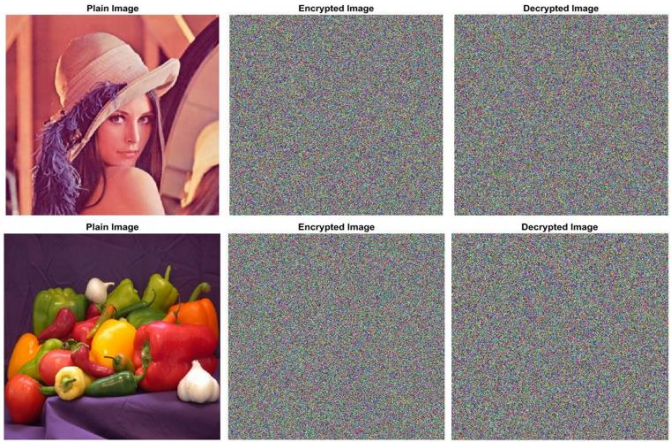

Fig. 13. Encryption and decryption of Lena and peppers color images with size 512 × 512. A, plain images, B, encrypted images and C, encrypted images

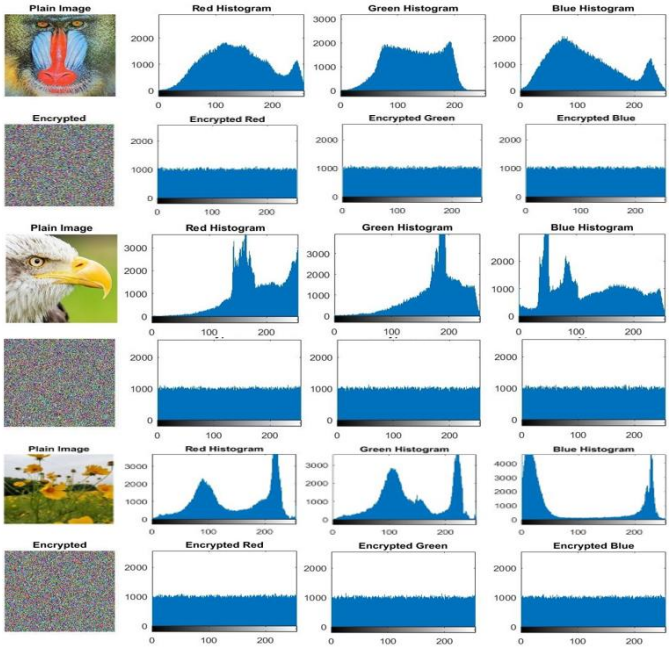

Fig. 14. Plain image and encrypted image with a histogram for each channel

TABLE II. INFORMATION ENTROPY TEST RESULTS FOR THE PROPOSED SYSTEM FOR NINE TEST IMAGES

Image Name	Red	Green	Blue	RGB
Lena	7.9993	7.9993	7.9994	7.9998
Peppers	7.9992	7.9993	7.9993	7.9997
Baboon	7.9993	7.9992	7.9994	7.9998
Barbara	7.9993	7.9993	7.9993	7.9998
Bird	7.9993	7.9992	7.9993	7.9998
Camel	7.9993	7.9992	7.9993	7.9998
Satellite image	7.9993	7.9993	7.9994	7.9998
Flower	7.9993	7.9994	7.9993	7.9997
Tree	7.9994	7.9992	7.9993	7.9998

TABLE III. COMPARING THE RESULTS OF THE PROPOSED SYSTEM ENTROPY TESTS WITH OTHER METHODS

Image	Lena			Tree			Flower		
	R	G	B	R	G	B	R	G	B
Ref [18]	7.9895	7.9792	7.9577	NA	NA	NA	NA	NA	NA
Ref [45]	7.9893	7.9898	7.9894	NA	NA	NA	NA	NA	NA
Ref [46]	NA	NA	NA	7.9898	7.9980	7.9892	7.9978	7.9864	7.9846
Proposed	7.9993	7.9993	7.9994	7.9994	7.9992	7.9993	7.9993	7.9994	7.9993

TABLE IV. NPCR AND UACI DATA

Images	Lena	Peppers	Baboon	Barbara	Bird	Camel	Satellite	Flower	Tree
NPCR	99.61%	99.60%	99.61%	99.61%	99.61%	99.61%	99.60%	99.60%	99.62%
UACI	30.36%	33.96%	31.76%	32.76%	32.45%	31.98%	33.19%	34.70%	31.28%

TABLE V. CORRELATION COEFFICIENTS FOR DIFFERENT DIRECTIONS OF TEST IMAGES

Direction	**Vertical**		**Horizontal**		**Diagonal**	
Image Type	**Plain**	**Cipher**	**Plain**	**Cipher**	**Plain**	**Cipher**
Lena	0.9747	-0.0299	0.9835	-0.0121	0.9762	-0.0477
Peppers	0.9929	0.0263	0.9940	0.0096	0.9871	-0.0047
Baboon	0.9273	-0.0383	0.9286	-0.0123	0.8360	-0.0130
Barbara	0.9482	0.0016	0.9442	-0.0125	0.9200	0.0033
Bird	0.9889	-0.0112	0.9918	0.0072	0.9831	-0.0099
Camel	0.9815	-0.0116	0.9859	-0.0037	0.9663	0.0053
satellite image	0.7970	-0.0231	0.8079	0.0053	0.6768	-0.0036
Flower	0.9926	-0.0001	0.9967	-0.0018	0.9897	0.0127
Tree	0.9835	0.0448	0.9822	0.0072	0.9653	-0.0241

TABLE VI. THE CORRELATION COEFFICIENTS COMPARISON OF THE PROPOSED METHOD WITH REF [20], REF [53] AND REF [55] USING LENA IMAGE

Direction	**Vertical**	**Horizontal**	**Diagonal**
Ref [20]	−0.0296	-0.0050	−0.0230
Ref [53]	0.00014	-0.00368	-0.02298
Ref [55]	0.0016	-0.0088	-0.0254
proposed	-0.0299	-0.0121	-0.0477

X. DISCUSSION AND REAL IMPLEMENTATION

The analysis and simulations were performed under the same conditions on the same device, Lenovo Windows 10 Pro; Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.59GHz, RAM: 16GB. The results of the chaotic properties tests showed that the proposed system has high chaotic behavior and new dynamics. Moreover, the results of the encrypted images are very close to the optimum value. Thus, the proposed image encryption algorithm is significantly very secure and has a high resistance to differential attacks. On the other hand, comparisons with other encryption algorithms based on chaotic systems showed very strong competition and high superiority of the proposed chaotic system and the encryption algorithm. According to the above findings, it is clear, the proposed system is trustworthy for most of the communications and data security needs.

XI. CONCLUSIONS

This paper proposed 3D discrete chaotic map, in order to design a high quality chaotic randomness with a long period length. The efficiency of the complex dynamics of the proposed system was analyzed by investigating the main characteristics of phase portraits, Lyapunov Exponent, 0 - 1 and randomness tests, and proved to be chaotic with outstanding performance. These statistical tests show that the encrypted images obtained from the proposed algorithm provide better protection against statistical and differential attacks. Moreover, the synchronization test confirmed the suitability of the proposed system for designing strong encryption algorithms and secure transmission systems in real environments, due to which synchronization occurs in a very short time. As a result, the proposed chaotic map is suitable for enhancing security and thwarting potential attacks and reliable for real-world application. To demonstrate the application of the proposed system, this paper presented a new algorithm based on known confusion and diffusion processes. The key stream depends on the initial condition and the propose scheme possesses high key sensitivity. The used security measurements and simulation analysis showed that the proposed algorithm possesses strong encryption procedures and high computational speed, and can overcome common weaknesses found in cryptographic algorithms based on chaotic systems.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENTS

The authors would like to thank the Iraqi Commission for Computer and Informatics, as well as the Informatics Institute for Post Grad, for their help and encouragement in performing this work.

REFERENCES

[1] Wen, J., Feng, Y., Tao, X., & Cao, Y. (2021). Dynamical analysis of a new chaotic system: Hidden attractor, coexisting-attractors, offset boosting, and DSP realization. *IEEE Access*, *9*, 167920-167927.

[2] Ma, C., Mou, J., Xiong, L., Banerjee, S., Liu, T., & Han, X. (2021). Dynamical analysis of a new chaotic system: asymmetric multistability, offset boosting control and circuit realization. *Nonlinear Dynamics*, *103*, 2867-2880.

[3] O'sullivan, A. M., O'callaghan, Y. C., O'grady, M. N., Hayes, M., Kerry, J. P., & O'brien, N. M. (2013). The effect of solvents on the antioxidant activity in Caco-2 cells of Irish brown seaweed extracts prepared using accelerated solvent extraction (ASE®). *Journal of Functional Foods*, *5*(2), 940-948.

[4] Muthu, J. S., & Murali, P. (2021). A new chaotic map with large chaotic band for a secured image cryptosystem. *Optik*, *242*, 167300.

[5] Sahari, M. L., & Boukemara, I. (2018). A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. *Nonlinear Dynamics*, *94*, 723-744.

[6] Kadhim, K. A., Adnan, M. M., Waheed, S. R., & Alkhayyat, A. (2021). Withdrawn: Automated high-security license plate recognition system.

[7] Waheed, S. R., Suaib, N. M., Rahim, M. S. M., Adnan, M. M., & Salim, A. A. (2021, April). Deep learning algorithms-based object detection and localization revisited. *Journal of Physics: Conference Series* (Vol. 1892, No. 1, p. 012001). IOP Publishing.

[8] Waheed, S. R., Saadi, S. M., Rahim, M. S. M., Suaib, N. M., Najjar, F. H., Adnan, M. M., & Salim, A. A. (2023). Melanoma skin cancer classification based on CNN deep learning algorithms. *Malaysian Journal of Fundamental and Applied Sciences*, *19*(3), 299-305.

[9] Ansari, S., Gupta, N., & Agrawal, S. (2012). A Review on chaotic map based cryptography. *International Journal of Scientific Engineering and Technology*, *1*(4), 24-27.

[10] Waheed, S. R., Rahim, M. S. M., Suaib, N. M., & Salim, A. A. (2023). CNN deep learning-based image to vector depiction. *Multimedia Tools and Applications*, 1-20.

[11] Salim, A. A., Ghoshal, S. K., Suan, L. P., Bidin, N., Hamzah, K., Duralim, M., & Bakhtiar, H. (2018). Liquid media regulated growth of cinnamon nanoparticles: Absorption and emission traits. *Malaysian Journal of Fundamental and Applied Sciences*, *14*(3-1), 447-449.

[12] Salim, A. A., Bakhtiar, H., Shamsudin, M. S., Aziz, M. S., Johari, A. R., & Ghoshal, S. K. (2022). Performance evaluation of rose bengal dye-decorated plasmonic gold nanoparticles-coated fiber-optic humidity sensor: A mechanism for improved sensing. *Sensors and Actuators A: Physical*, *347*, 113943.

[13] Vaseghi, B., Mobayen, S., Hashemi, S. S., & Fekih, A. (2021). Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption. *IEEE Access*, *9*, 25911-25925.

[14] Durdu, A., Uyaroğlu, Y., & Özcerit, A. T. (2015). A novel chaotic system for secure communication applications. *Information Technology and Control*, *44*(3), 271-278.

[15] Pecora, L. M., & Carroll, T. L. (1991). Synchronization in chaotic circuits. *IEEE Trans. Circuit Syst*, *38*, 453.

[16] Abdullah, H. A., & Abdullah, H. N. (2018). A new chaotic map for secure transmission. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *16*(3), 1135-1142.

[17] Abdullah, H. N., & Abdullah, H. A. Four-dimensional Tinkerbelle chaotic system for secure transmission.

[18] Jovic, B. (2011). *Synchronization techniques for chaotic communication systems*. Springer Science & Business Media.

[19] Zolfaghari-Nejad, M., Charmi, M., & Hassanpoor, H. (2022). A new chaotic system with only nonhyperbolic equilibrium points: Dynamics and its engineering application. *Complexity*, *2022*, 1-16.

[20] Abdullah, H. A., Abdullah, H. N., & Mahmoud Al-Jawher, W. A. (2020). A hybrid chaotic map for communication security applications. *International Journal of Communication Systems*, *33*(4), e4236.

[21] Dong, C. (2022). Dynamics, periodic orbit analysis, and circuit implementation of a new chaotic system with hidden attractor. *Fractal and Fractional*, *6*(4), 190.

[22] Farajallah, M. (2015). Chaos-based crypto and joint crypto-compression systems for images and videos. Doctoral dissertation, Universite de Nantes.

[23] Salim, A. A., Bakhtiar, H., & Ghoshal, S. K. (2021). Improved fluorescence quantum yield of nanosecond pulse laser ablation wavelength controlled cinnamon nanostructures grown in ethylene glycol medium. *Optik*, *244*, 167575.

[24] Liu, Y., Fan, H., Xie, E. Y., Cheng, G., & Li, C. (2014). Deciphering a novel image cipher based on mixed transformed Logistic maps. *arXiv preprint arXiv:1404.3600*.

[25] Salim, A. A., Bidin, N., Ghoshal, S. K., Islam, S., & Bakhtiar, H. (2018). Synthesis of truncated tetrahedral cinnamon nanoparticles in citric acid media via PLAL technique. *Materials Letters*, *217*, 267-270.

[26] Hénon, M. (2004). A two-dimensional mapping with a strange attractor. *The theory of chaotic attractors*, 94-102.

[27] Salim, A. A., Bidin, N., & Islam, S. (2017). Low power CO_2 laser modified iron/nickel alloyed pure aluminum surface: Evaluation of structural and mechanical properties. *Surface and Coatings Technology*, *315*, 24-31.

[28] Li, W., Wang, C., Feng, K., Huang, X., & Ding, Q. (2018). A multidimensional discrete digital chaotic encryption system. *International Journal of Distributed Sensor Networks*, *14*(9), 1550147718802781.

[29] Wang, C., Di, Y., Tang, J., Shuai, J., Zhang, Y., & Lu, Q. (2021). The dynamic analysis of a novel reconfigurable cubic chaotic map and its application in finite field. *Symmetry*, *13*(8), 1420.

[30] Sándor, Z., & Maffione, N. (2016). The relative Lyapunov indicators: Theory and application to dynamical astronomy. *Chaos Detection and Predictability*, 183-220.

[31] Kadhim, K. A., Najjar, F. H., Waad, A. A., Al-Kharsan, I. H., Khudhair, Z. N., & Salim, A. A. (2023). Leukemia classification using a convolutional neural network of AML images. *Malaysian Journal of Fundamental and Applied Sciences*, *19*(3), 306-312.

[32] Gottwald, G. A., & Melbourne, I. (2016). The 0-1 test for chaos: A review. *Chaos detection and predictability*, 221-247.

[33] Aldhuhaibat, M. J., Amana, M. S., Aboud, H., & Salim, A. A. (2022). Radiation attenuation capacity improvement of various oxides via high density polyethylene composite reinforcement. *Ceramics International*, *48*(17), 25011-25019.

[34] Salim, A. A., Bidin, N., Bakhtiar, H., Ghoshal, S. K., Al Azawi, M., & Krishnan, G. (2018, May). Optical and structure characterization of cinnamon nanoparticles synthesized by pulse laser ablation in liquid (PLAL). *Journal of Physics: Conference Series* (Vol. 1027, No. 1, p. 012002). IOP Publishing.

[35] Patidar, V., Sud, K. K., & Pareek, N. K. (2009). A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Informatica*, *33*(4).

[36] Salim, A. A., Ghoshal, S. K., & Bakhtiar, H. (2021). Growth mechanism and optical characteristics of Nd: YAG laser ablated amorphous cinnamon nanoparticles produced in ethanol: Influence of accumulative pulse irradiation time variation. *Photonics and Nanostructures-Fundamentals and Applications*, *43*, 100889.

[37] Boccaletti, S., Kurths, J., Osipov, G., Valladares, D. L., & Zhou, C. S. (2002). 10.1016/s0370-1573 (02) 00137-0. *Phys. Rep*, *366*, 1-101.

[38] Iqbal, N., Naqvi, R. A., Atif, M., Khan, M. A., Hanif, M., Abbas, S., & Hussain, D. (2021). On the image encryption algorithm based on the chaotic system, dna encoding, and castle. *IEEE Access*, *9*, 118253-118270.

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

[40] Bashir, Z., Iqbal, N., & Hanif, M. (2021). A novel gray scale image encryption scheme based on pixels' swapping operations. *Multimedia Tools and Applications*, *80*, 1029-1054.

[41] Qian, X., Yang, Q., Li, Q., Liu, Q., Wu, Y., & Wang, W. (2021). A novel color image encryption algorithm based on

three-dimensional chaotic maps and reconstruction techniques. *IEEE Access*, *9*, 61334-61345.

[42] Emam, S. A., & Abdalla, M. M. (2015). Subharmonic parametric resonance of simply supported buckled beams. *Nonlinear Dynamics*, *79*, 1443-1456.

[43] Zhang, D., Chen, L., & Li, T. (2021). Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation. *Entropy*, *23*(3), 361.

[44] Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A. M., & Mirnia, M. (2021). A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and Applications*, *80*, 2753-2772.

[45] Amana, M. S., Muslim, R. I., Aldhuhaibat, M. J., & Salim, A. A. (2021). Assessment of Radiation Levels and Geochemical Factors in Iraqi Soil. *NeuroQuantology*, *19*(6), 79.

[46] Salim, A. A., Ghoshal, S. K., Danmallam, I. M., Sazali, E. S., Krishnan, G., Aziz, M. S., & Bakhtiar, H. (2021, April). Distinct optical response of colloidal gold-cinnamon nanocomposites: Role of pH sensitization. *Journal of Physics: Conference Series (Vol. 1892*, No. 1, p. 012039). IOP Publishing.

[47] Waheed, S. R., Sakran, A. A., Rahim, M. S. M., Suaib, N. M., Najjar, F. H., Kadhim, K. A., Salim, A. A. & Adnan, M. M. (2023). Design a Crime Detection System based Fog Computing and IoT. *Malaysian Journal of Fundamental and Applied Sciences*, *19*(3), 345-354.

[48] Rehman, M. U., Shafique, A., Khalid, S., & Hussain, I. (2021). Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps. *IEEE Access*, *9*, 52277-52291.

[49] Khalil, N., Sarhan, A., & Alshewimy, M. A. (2021). An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Optics & Laser Technology*, *143*, 107326.

[50] Wang, X., Guan, N., & Yang, J. (2021). Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map. *Chaos, Solitons & Fractals*, *150*, 111117.

[51] Ngo, T. D., Bui, T. T., Pham, T. M., Thai, H. T., Nguyen, G. L., & Nguyen, T. N. (2021). Image deconvolution for optical small satellite with deep learning and real-time GPU acceleration. *Journal of Real-Time Image Processing*, *18*(5), 1697-1710.

[52] Wu, X., Li, Y., & Kurths, J. (2015). A new color image encryption scheme using CML and a fractional-order chaotic system. *PloS one*, *10*(3), e0119660.

[53] Hu, W., & Dong, Y. (2022). Quantum color image encryption based on a novel 3D chaotic system. *Journal of Applied Physics*, *131*(11), 114402.

[54] Bouteghrine, B., Tanougast, C., & Sadoudi, S. (2021). Novel image encryption algorithm based on new 3-d chaos map. *Multimedia Tools and Applications*, *80*, 25583-25605.

[55] Abdul-Kareem, A. A., & Al-Jawher, W. A. M. (2022). Uruk 4D discrete chaotic map for secure communication applications. *Journal Port Science Research*, *5*(3), 131-142.