j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

URUK 4D DISCRETE CHAOTIC MAP FOR SECURE COMMUNICATION APPLICATIONS

Ali. A. Abdul-Kareem*[1], Waleed A. M. Al-Jawher[2]

[1] *Iraqi Commission for Computers and Informatics, Information Institute for Postgraduate Studies, Baghdad, Iraq..*
phd202020559@iips.icci.edu.iq
[2]*College of Engineering, Uruk University, Baghdad, Iraq.*
profwaleed54@gmail.com

Abstract In this paper, URUK, a discrete four-dimensional chaotic map, is proposed for secure communication. The 0-1 tests, the Lyapunov Exponent (LE) tests, and the National Institute of Standard and Technology (NIST) tests, which are typically used to verify the randomness of bits, are employed to evaluate the dynamic behavior of the system based on a variety of criteria. Based on the results of tests demonstrating the system's characteristic chaotic and random behavior, it is reliable for use in covert communications and image encryption.

Crossref 10.36371/port.2022.3.2

Keywords: *Chaos, Chaotic system, Discrete Chaotic Map, URUK, Image Encryption, Secure Communication*

1. INTRODUCTION

In recent years, the scientific community has paid a great deal of attention to the physical phenomenon that chaos is highly sensitive to the initial value, as researchers have exploited this phenomenon in dynamical systems to establish a close connection between chaotic systems and secure communication applications [1]. As research progressed, the use of chaotic systems expanded to new fields of application, gaining notoriety not only among computer scientists, but also among economists, physicists, engineers, and biologists [3, 4]. Simulating different chaotic phenomena, proposing new chaotic methods, hybridizing two or more chaotic maps, enhancing existing chaotic methods, and synchronizing two or more chaotic systems were all encouraged by the equations' simplicity, application versatility, and low computational complexity [4]. In order to implement a robust security system, it is always necessary to create a new dynamic system for synchronization and data encryption. Wang et al. [1] proposed a new chaotic four-dimensional system by modifying the Wei system. The system has fixed equilibrium points, subtle attractors, and complex dynamic phenomena, such as the symbiosis of periodic windows and attractors. Abdul-Kareem et al [4] proposed WAM, a novel 3D discrete chaotic map. To encrypt data and ensure secure communication. This system generates a rich dynamic with some intriguing initial condition and parameter-related properties. Wen et al [5] presented a chaotic five-dimensional system with a hidden attractor. The system is distinguished by the ease with which it can generate hidden chaotic attractors with extremely large static conditions, as well as its complex dynamic behavior, which makes it suitable for secure communication and image encryption. Dong [6] described a new autonomous chaotic system with two stable node-foci capable of producing double-wing hidden chaotic attractors by modifying a simple three-dimensional continuous quadratic dynamical system. Rahman et al. [7] proposed a new fractional order chaotic system devoid of equilibrium. Due to its lack of equilibrium, it has the ability to elicit subtle, untidy attractants. Between two identical new systems, a synchronization mechanism based on the adaptive control theory was developed (master and slave). The adaptive control laws are derived from the synchronization error dynamics of the master and slave state variable systems. Chenguang et al. [8] designed a new four-dimensional dissipative chaotic system that is capable of generating multiple asymmetric attractors. The significance of the discoveries in the aforementioned systems motivates us to pursue the same course of action. This study introduces a new chaotic system for securing communication data. Using 0-1 tests, Lyapunov exponents, and phase portraits, the randomness performance of the proposed system was

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

analyzed. The remainder of this research is organized as follows. The second section provides a detailed description of the proposed discrete chaotic 4D map. The third section presents a comparison of bit-stream generators and the results of several tests conducted on the proposed chaotic system. Finally, the proposed system is implemented in the image encryption algorithm in order to demonstrate its efficacy.

2. THE PROPOSED URUK 4D DISCRETE CHAOTIC SYSTEM

Both discrete and continuous classifications of chaotic systems contain both one-dimensional and multidimensional maps. Due to their simple structure, low-dimensional chaotic maps are simple to implement, but their dynamic degradation frequently deviates significantly from theoretical expectations. Multidimensional maps, on the other hand, make it more challenging to predict the chaotic path, which is highly desirable in secure communication. As a result, the novel concept presented in this paper is to propose a new discrete chaotic map in four dimensions, dubbed Uruk

$$X_{(n+1)} = 1 - (X_n \times Y_n \times Z_n \times W_n) - X_n^2 - Y_n^2 - a \times \tan(Z_n^2) - W_n^2 \quad (1)$$

$$Y_{(n+1)} = X_n - b \times \tan(Z_n) \quad (2)$$

$$Z_{(n+1)} = Y_n - c \times \tan(Z_n) \quad (3)$$

$$W_{(n+1)} = X_n - d \times W_n \quad (4)$$

The system variables are x, y, z, and w, while the bifurcation states are a, b, c, and d. Adding trigonometric functions and nonlinear terms to the preceding equations increases the randomness of the proposed discrete chaotic 4D Uruk system. The 3D projections of the phase images of the proposed system were obtained with the control parameters a = 0.05, b = 0.05, c = 0.05, and d = 0.05, and the system variables used were X (0) = 0.3, Y (0) = 0.2, Z (0) = 0.1, and W (0) = 0.4 as shown in Figure (1). The peculiar shape of the attractors suggests that the Uruk system exhibits strong chaotic behavior and a variety of complex dynamic properties.

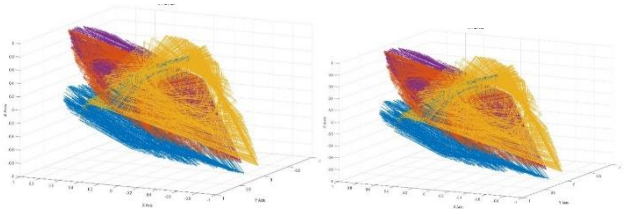


Figure 1*: The 4D discrete chaotic map phase portraits*

3. EXPERIMENTAL ANALYSIS

Several statistical tests have been conducted on the proposed map to confirm that it is capable of producing numerical strings that meet the chaotic criteria. The proposed system dynamics are illustrated in Figure 2. From this plot of signal amplitude versus time, it is evident that the probability distribution of all values is constant, meaning that the probability of producing any random number remains unchanged under the proposed system's dynamics. This initial result demonstrates the chaotic nature of the 4D map of Uruk.

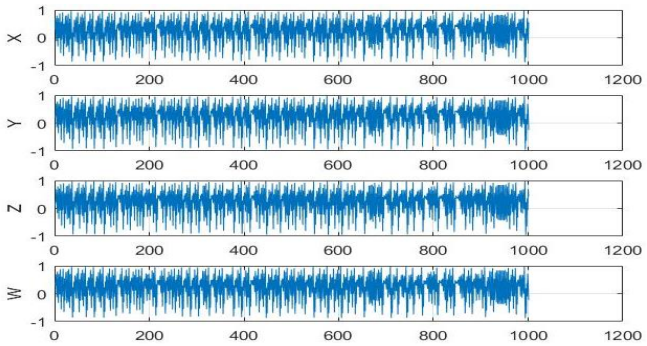


Figure 2: *Waveforms of Uruk 4D discrete chaotic map*

3.1. Behavior Analysis of The Proposed Discrete 4D Chaotic System

To determine whether the Uruk 4D system exhibited chaotic behavior, the Lyapunov Exponent (LE) test was applied. This is one of the most widely used tests for determining whether a system exhibits chaotic behavior. In general, to demonstrate the disorder of a system, at least one value must be positive; the system is periodic when LE is negative, and bifurcation has occurred when LE is zero [9, 10]. During the application of the Lyapunov Exponent (LE) test, the Jacobian matrix was used

$-2 \times x - w \times y \times z$	$-2 \times y - w \times x \times z$	$-2 \times a \times z \times (tan(z\text{^}2)\text{^}2 + 1) - w \times x \times y$	$-1/(5 \times w\text{^}(4/5)) - x \times y \times z$
1	0	$-b \times (tan(z)\text{^}2 + 1)$	0
0	1	$-c \times (tan(z)\text{^}2 + 1)$	0
1	0	0	$-d$

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

The above equation yielded the following result: LE1 = 0.033, LE2 = 0.018, LE3 = -0.162, LE4= -0.200 and Lyapunov dimension, 2.3109. A positive result indicates that the proposed system possesses chaotic properties. Figure 4 demonstrates every calculated Lyapunov exponent (LE).

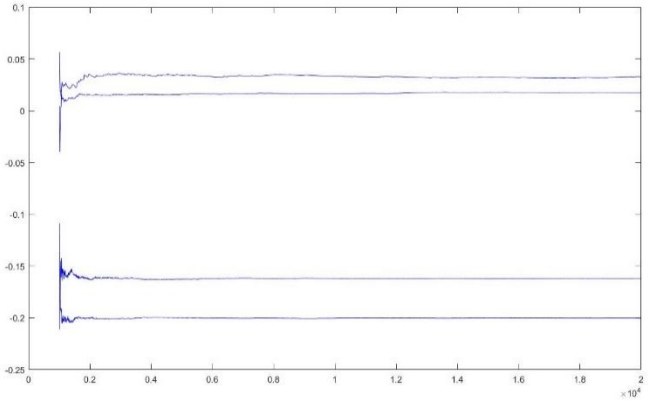


Figure 3: *Lyapunov Exponents (LE) of Uruk 4D discrete system*

3.2. Zero-One Test

Gottwald and Melbourne [11] and [12] introduced the zero-one test to distinguish between periodic and chaotic behavior in dynamical systems. The following steps are taken during the 01 test:

1. Consider the test input to be D(n), a one-dimensional time series with n = 1, 2, 3,..., N.
2. Define R as a positive and real number.
3. Determine the translation variables p(n+1) and q(n+1) as follows:

$$p(n+1) = p(n) + D(n)\cos(nR) \qquad (5)$$

$$q(n+1) = q(n) + D(n)\sin(nR) \qquad (6)$$

4. Use the equation (7) to calculate mean square displacement (MSD).

$$MSD(n) = \lim_{n\to\infty} \frac{1}{N} \sum_{j=1}^{N} ([p(j+n) - p(j)]^2 + [q(j+n) - q(j)]^2) \qquad (7)$$

5. Lastly, calculate the approximation growth average (K) using the equation below:

$$K = \lim_{n\to\infty} \frac{\log MSD(n)}{\log n} \qquad (8)$$

The value of K in deterministic systems must be close to 1 for chaos, whereas chaotic behavior disappears when K equals zero [10-12]. Kx = 0.9982, Ky = 0.9981, Kz = 0.9981 and Kw = 0.9980 are the K values that are obtained for the variables of the URUK system. These results demonstrate the chaotic properties of the proposed discrete 4D chaotic system, as the system is nearly transparent to 1.

3.3. Autocorrelation Function

The autocorrelation function is one of the most widely used tools for measuring the stochastic property of multidimensional chaotic systems by measuring the signal's self-similarity across various delay times [13]. Figure (4) depicts an autocorrelation function that appears semi-flat, indicating that the chaotic sequences generated by the proposed 4D discrete chaotic system are trustworthy for use in secure communications applications.

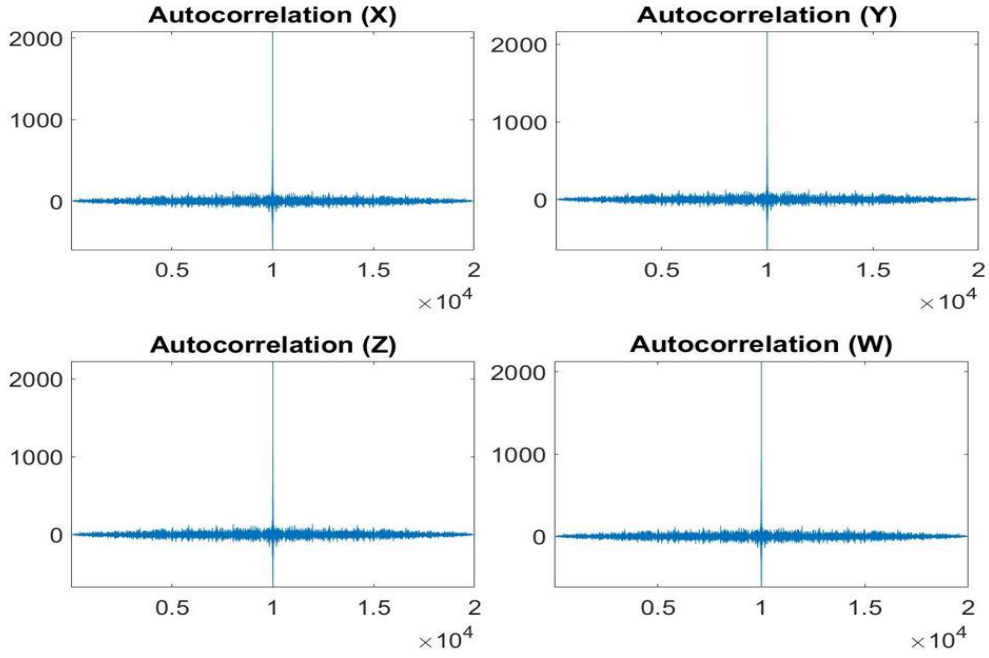


Figure 4: *depicts the autocorrelation function for each component of the URUK 4D discrete chaotic system*

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

Due to the significance of binary streams in cryptographic algorithms, the chaotic strings generated by the Uruk system are converted into independent random binary streams by matching two chaotic systems with the same control parameters but different initial conditions. The parameters employed are (a = 0.05, b = 0.05, c = 0.05, and w = 0.05), and the initial system values are (X1 = 0.3, Y1 = 0.2, Z1 = 0.1, W1 = 0.4, X2 = 0.2 and Y2 = 0.1 and Z2 = 0.2 and W2 = 0.3). Figure (5) depicts how chaotic systems were matched using equations (9-12):

$$BX=\begin{cases}1, & if \quad X2 < X1\\ 0, & if \quad X2 \geq X1\end{cases} \text{ where } X_1(0) \neq X_2(0) \qquad (9)$$

$$BY=\begin{cases}1, & if \quad Y2 < Y1\\ 0, & if \quad Y2 \geq Y1\end{cases} \text{ where } Y_1(0) \neq Y_2(0) \qquad (10)$$

$$BZ=\begin{cases}1, & if \quad Z2 < Z1\\ 0, & if \quad Z2 \geq Z1\end{cases} \text{ where } Z_1(0) \neq Z_2(0) \qquad (11)$$

$$BW=\begin{cases}1, & if \quad W2 < W1\\ 0, & if \quad W2 \geq W1\end{cases} \text{ where } W_1(0) \neq W_2(0) \qquad (12)$$

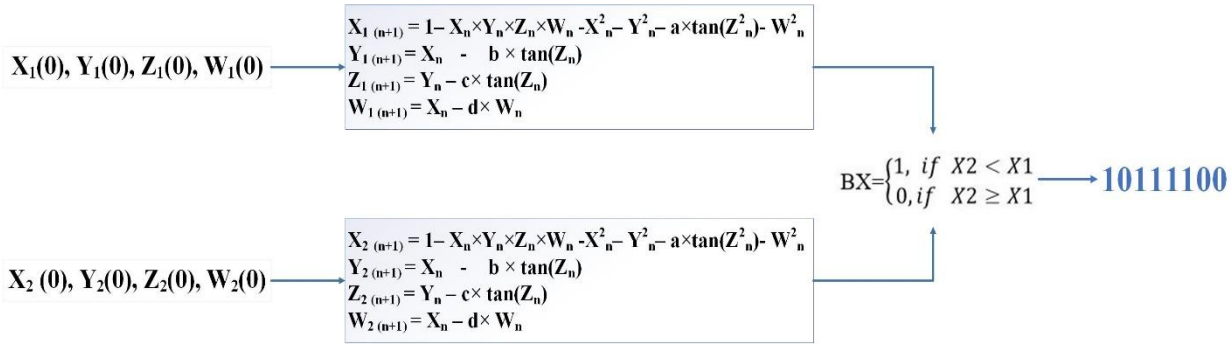


***Figure 5**: depicts the Generator of Random Binary Numbers*

3.4. The Randomness Tests

The stochastic properties of long binary sequences have been evaluated using a National Institute of Standards and Technology (NIST) test [2, 4, 14]. By accepting the null hypothesis, it has been demonstrated that the binary sequences generated by the proposed discrete 4D chaotic system are completely random. The NIST test results are presented in Table (1). This table demonstrates that all test values are very encouraging, indicating that the proposed 4D discrete chaotic system has optimal encryption properties and can therefore be used to create new stream ciphers.

***Table 1.** The National Institute of Standards and Technology (NIST) test outcomes.*

The Randomness Tests	BX	BY	BZ	BW	Evaluation
Frequency (MonoBit) test	0.8495	0.9999	0.8495	0.9496	Passed
Frequency (block = 1000) test	0.9274	0.9245	0.9435	0.9836	Passed
Run test	0.3382	0.5040	0.2033	0.2842	Passed
Longest run of ones	0.7820	0.1673	0.5837	0.1673	Passed
Binary matrix rank test	0.2919	0.2919	0.2919	0.2919	Passed
Discrete Fourier Transform (DFT) test	0.1468	0.2457	0.1468	0.2457	Passed
Maurer test	0.9421	0.8452	0.8340	0.9941	Passed
Approximate entropy test	0.7499	0.8598	0.7219	0.9219	Passed
Cumulative sum test – Forward	0.5899	0.6183	0.7656	0.7947	Passed
Cumulative sum test – Reverse	0.7656	0.6183	0.5899	0.8505	Passed
Non Overlapping Test	0.4215	0.5928	0.5267	0.7541	Passed

4. Simulation of Image Encryption Algorithm for Data Security

The proposed chaotic system is tested by generating an encryption key for an image encryption system in order to confirm its effectiveness. Initial values and control parameters for the Uruk 4D discrete chaotic system are X(1) = 0.3, Y(1) = 0.2, Z(1) = 0.1, W(1) = 0.4, a = 0.05, b = 0.05, c = 0.05, and d = 0.05. Several 512×512 color images, namely Lena, Barbara, Boats, Baboon, and Goldhill, are used to examine the various features of the proposed system. In the encryption system, the steps below are followed.

1. Create red, green, and blue channels from a color image by isolating its primary channels.
2. Convert each of the red, green, and blue channels to a one-dimensional vector in preparation for the confusion procedure.

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

3. The encryption key is generated by an equation-based Uruk 4D discrete chaotic system (1 - 4). For the proposed encryption method, only three chaotic sequences (X, Y, and Z) were used.
4. Based on the encryption key obtained from the proposed chaotic map, the pixel positions in each channel are confused.
5. Generate bit-stream by converting the proposed encryption key to its binary representation based on Equations (9-12). For the proposed encryption method, only three encryption keys (BX, BY, and BZ) were used.
6. Using the XOR operation, the pixel values of confused channels are diffused.

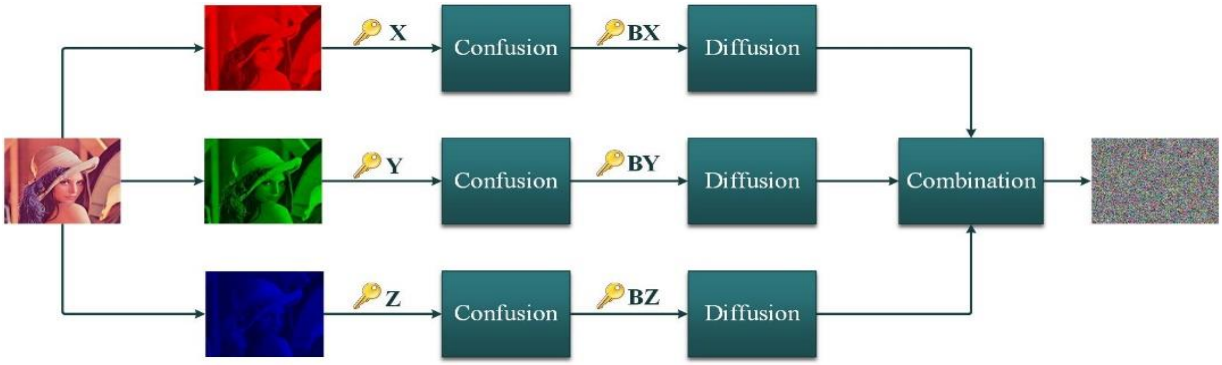


Figure 6: *illustrates the main block diagram for the proposed method.*

5. Evaluation of the Proposed Encryption System Using Statistics

Using statistical analysis, the encryption algorithms can be broken. To determine the effectiveness of the proposed method against statistical attacks, the pixel distribution of the encrypted image is studied using histogram analysis and the correlation coefficient.

5.1. The Correlation Coefficient

Normal image pixels are statistically related in the horizontal, vertical, and diagonal directions. In order to express this statistical relationship, correlation coefficient analysis is employed. In normal images, the correlation coefficient value is close to 1, whereas in encrypted images, the correlation coefficient value is close to 0. Here, the effect of efficient coding algorithms on the generation of an encrypted image with the lowest possible correlation becomes apparent [15-18]. Figure (7) illustrates the close statistical relationship between the pixels in the original image in all directions, where all pixels are concentrated in one area. Figure (8) depicts the random distribution of pixels in the encrypted image produced by the proposed method. The pixels are dispersed throughout the region.

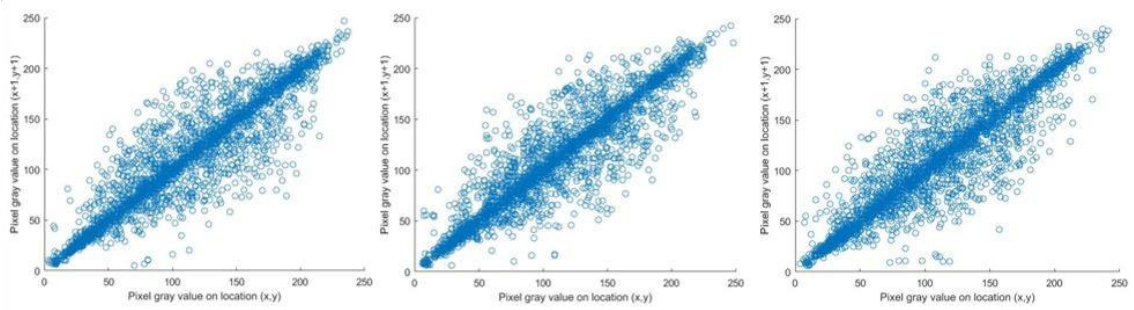


Figure 7*: displays the correlation coefficient of 3000 randomly chosen pixels in all directions of the Barbara image*

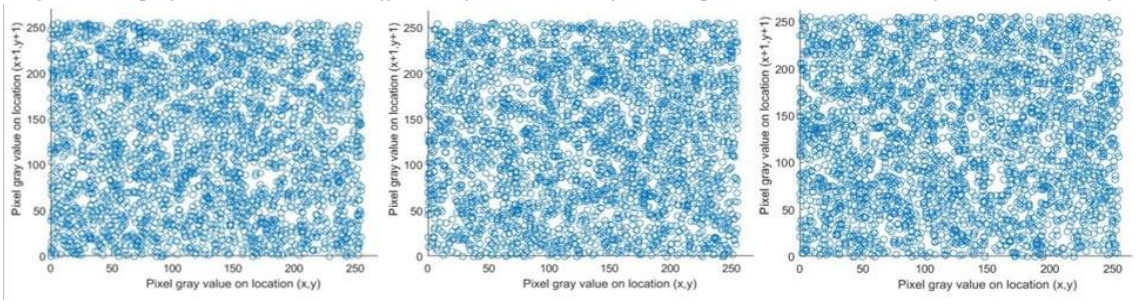


Figure 8*: displays the correlation coefficient of 3000 randomly chosen pixels in all directions of the ciphered Barbara image.*

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

***Table 2**. Correlation coefficients between test image pixels in the vertical, horizontal, and diagonal directions.*

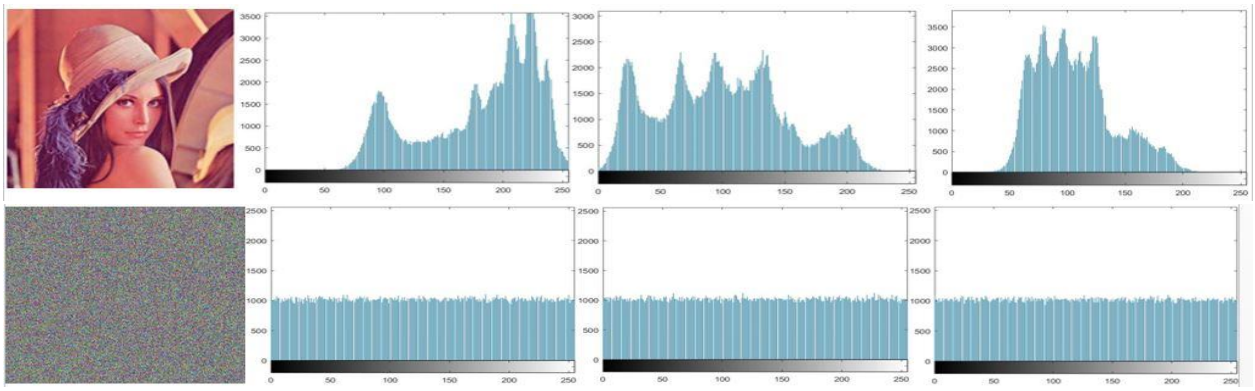
Direction	**Vertical**		**Horizontal**		**Diagonal**	
Image Type	Plain	Cipher	Plain	Cipher	Plain	Cipher
Lena	0.9773	-0.0312	0.9807	-0.0164	0.9732	-0.0262
Barbara	0.9333	-0.0152	0.9239	-0.0166	0.9200	0.0005
Boats	0.9715	0.0002	0.9739	-0.0049	0.9517	-0.0335
Baboon	0.9327	-0.0259	0.9301	-0.0215	0.8863	-0.0145
Gold-hill	0.9795	-0.0035	0.9793	0.0041	0.9676	-0.0238

***Table 3.** Compares the correlation coefficients of the proposed method to those of other methods using Lena images*

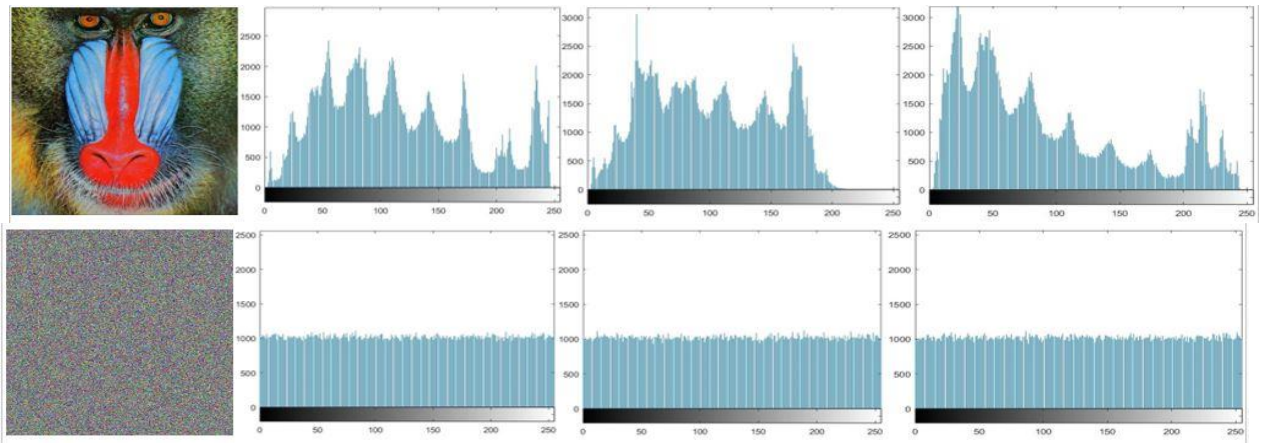
Direction	**Vertical**	**Horizontal**	**Diagonal**
Ref [2]	−0.0296	-0.0050	−0.0230
Ref [4]	-0.0299	-0.0121	-0.0477
Ref [18]	0.0016	-0.0088	-0.0254
proposed	-0.0312	-0.0164	-0.0262

5.2. The Pixels Distribution

Histogram analysis is one of the most crucial statistical tests for evaluating the resistance of encryption algorithms to statistical analysis attacks. Graphically describing the distribution of pixel density, the histogram provides a comprehensive description of the image's content. Consequently, the normal image histogram and the encrypted image histogram must be fundamentally distinct, with the normal image histogram containing multiple peaks and vertices and the encrypted image histogram being flat, which helps to conceal the pixel density distribution information from attackers [19-22]. Figure (9) depicts the histogram of the red, green, and blue channels of the normal and encrypted images generated by the proposed method, which demonstrated an effective outcome.



Plain and Encrypted Lena image

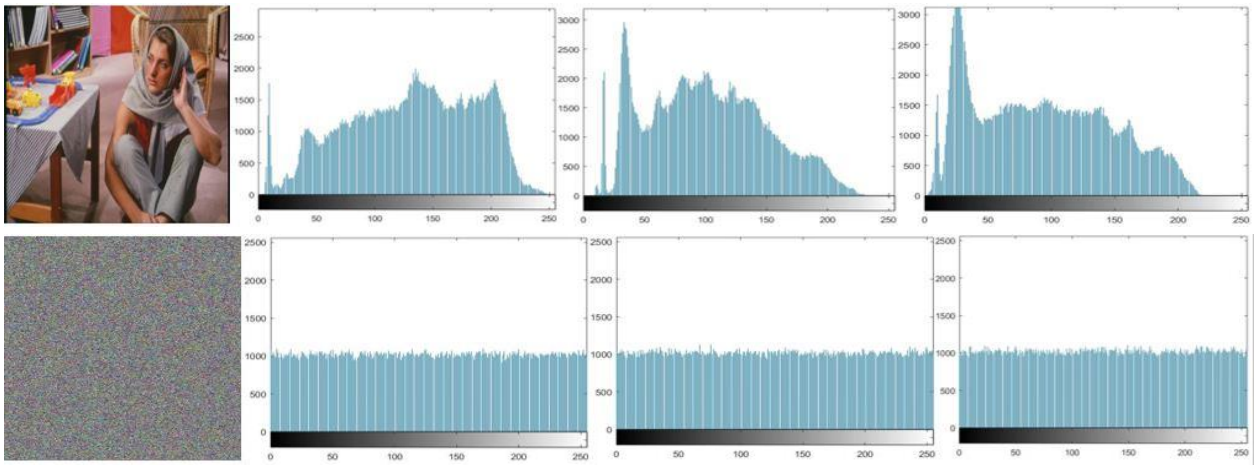


Plain and Encrypted Baboon image

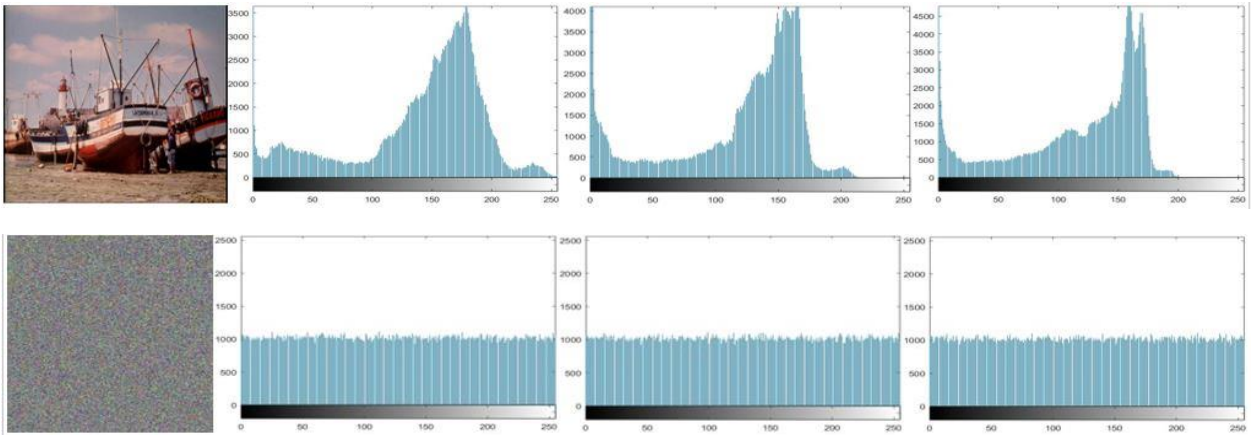
Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

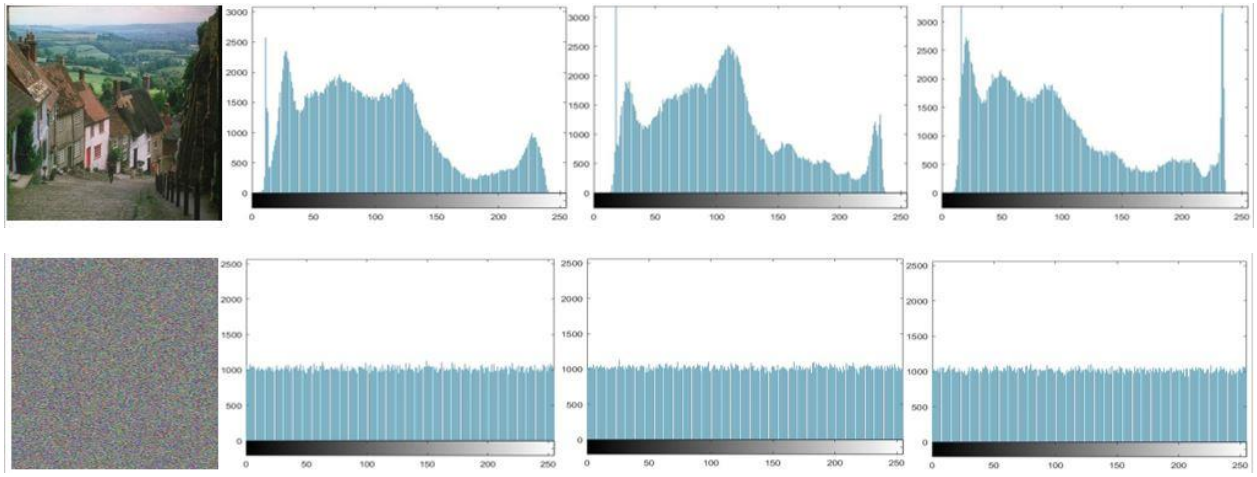
Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022



Plain and Encrypted Barbara image



Plain and Encrypted Boats image



Plain and Encrypted Gold-hill image

Figure 9: *shows the histogram for the red, green, and blue channels of the original and encrypted images.*

5.3. Examination of Information Entropy

The information entropy test was proposed by Shannon [23] in 1948 as an analytical measure for assessing the level of randomness in encrypted images. The results of this test range from 0 to 8 for images with pixel values between 0 and 255, and the entropy scale score for encrypted images is approximately eight, indicating that the encryption algorithm is effective at repelling the entropy attack. If the entropy is significantly less than the maximum value, however, the encoded image is ineffective and cannot withstand an entropy

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

attack [24-27]. The following formula is used to calculate entropy:

$$IE(S) = -\sum P(S) \times Log_2\, P(S) \qquad (13)$$

The average entropy value in Table (2) is close to 8, indicating that encrypted images have the potential to thwart an information entropy attack. In comparison to encryption methods based on other chaotic systems, the encryption algorithm based on the Uruk four-dimensional chaotic map demonstrates superior performance and competitive results in Table (3).

Table 4. *Entropy information examination results for five test images using the proposed chaotic system.*

Image Name	Red	Green	Blue	RGB
Lena	7.9993	7.9993	7.9994	7.9998
Barbara	7.9993	7.9993	7.9993	7.9998
Boats	7.9993	7.9992	7.9992	7.9998
Baboon	7.9994	7.9993	7.9993	7.9998
Gold-hill	7.9992	7.9993	7.9993	7.9997

Table 5*. Comparing the evaluation results of the proposed chaotic map to those of other method*

Image	Lena			Baboon		
	R	G	B	R	G	B
Ref [2]	7.9895	7.9792	7.9577	NA	NA	NA
Ref [4]	7.9993	7.9993	7.9994	7.9993	7.9992	7.9994
Ref [28]	7.9993	7.9994	7.9993	7.9992	7.9993	7.9993
Ref [29]	7.9973	7.9975	7.9975	7.9970	7.9972	7.9972
Proposed	7.9993	7.9993	7.9994	7.9994	7.9993	7.9993

5.4. Assessing the algorithm's resistance to differential attack

S A differential attack involves determining the key and the cryptographic system by tracing the meaningful relationships between the original and encrypted images. In response to any change, regardless of size, in the original image, high-impact encryption algorithms modify the encrypted image significantly. Modifying at least one pixel in one of the two original images and comparing the differences between the two encoded images determines the sensitivity and resistance of the encoded image to differential attacks [30, 31]. The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are determined through the equations (14) and (15):

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \text{image}(i,j) \times 100\% \qquad (14)$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\text{Encrypted1} - \text{Encrypted2}}{255} \times 100\% \qquad (15)$$

In addition, Table (6) displays the outcomes of the NPCR and UACI analyses, which demonstrate that the proposed algorithm is highly sensitive and resistant to differential attacks.

Table 6. *NPCR and UACI data.*

Images	Lena	Barbara	Boats	Baboon	Gold-hill
NPCR	99.61	99.60	99.61	99.61	99.58
UACI	33.32	33.21	33.41	33.31	33.32

5.5. Key Sensitivity Analysis

A very small change in the initial conditions will result in a large change in the output, as the encryption algorithm employs a four-dimensional chaotic map that is extremely sensitive to any change in initial conditions. To test the sensitivity of the Uruk chaotic map, the control parameters of the decryption key were modified in a straightforward manner. Initially, the original image is encrypted with a valid key obtained by repeating the URUK chaotic map N * N times and using the following initial values: X(1) = 0.3, Y(1) = 0.2, Z(1) = 0.1, W(1) = 0.4, a = 0.05, b = 0.05, c = 0.05, and d = 0.05. The image is then decrypted using the same conditions with the exception that the value of the initial state (a) is altered to 0.05000000001. Barbara's color image is displayed in Figure 10 as test images. Clearly, the decryption procedure with slightly altered initial conditions fails completely. Therefore, the secret key generated by the proposed chaotic system is extremely sensitive, indicating that the encrypted images produced by the proposed algorithm are resistant to brute-force attacks.

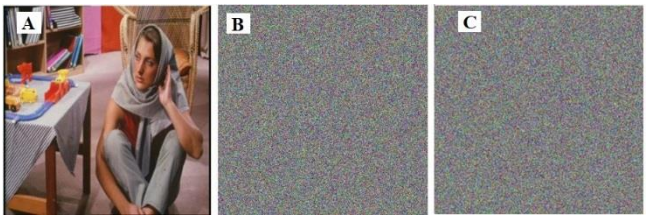


Figure 10: *depicts the encryption and decryption of a 512-by-512 Barbara test image. A, plain images, B, encrypted images and C, decrypted images.*

5.6. Noise attack evaluation

The noise pollution attack is one of the most prevalent in the cryptanalysis community; it targets sensitive images as they are an essential information carrier [33]. As a 512×512 test image for evaluating the robustness of the encryption algorithm based on Uruk secret keys, Barbara and Lena images were used. Table 7 displays the algorithm's security performance by displaying the PSNR values and the added noise intensity for each test. In addition, the decrypted images remained distinguishable despite being exposed to noise pollution attacks, demonstrating the algorithm's resistance to this type of attack.

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

***Table 7**: displays the PSNR and intensity of noise added to images of Bird and Lena*

Noise	**PSNR**	**Image**	**Original**	**0.000001**	**0.000003**	**0.000005**	**0.000007**
Salt and pepper	dB	Lena	Inf	Inf	Inf	Inf	Inf
		Barbara	Inf	Inf	Inf	Inf	Inf
Noise	**PSNR**	**Image**	**Original**	**0.000001**	**0.000002**	**0.000003**	**0.000004**
Speckle	dB	Lena	Inf	Inf	48.8295	41.1857	38.6123
		Barbara	Inf	Inf	48.7373	41.0877	38.4993

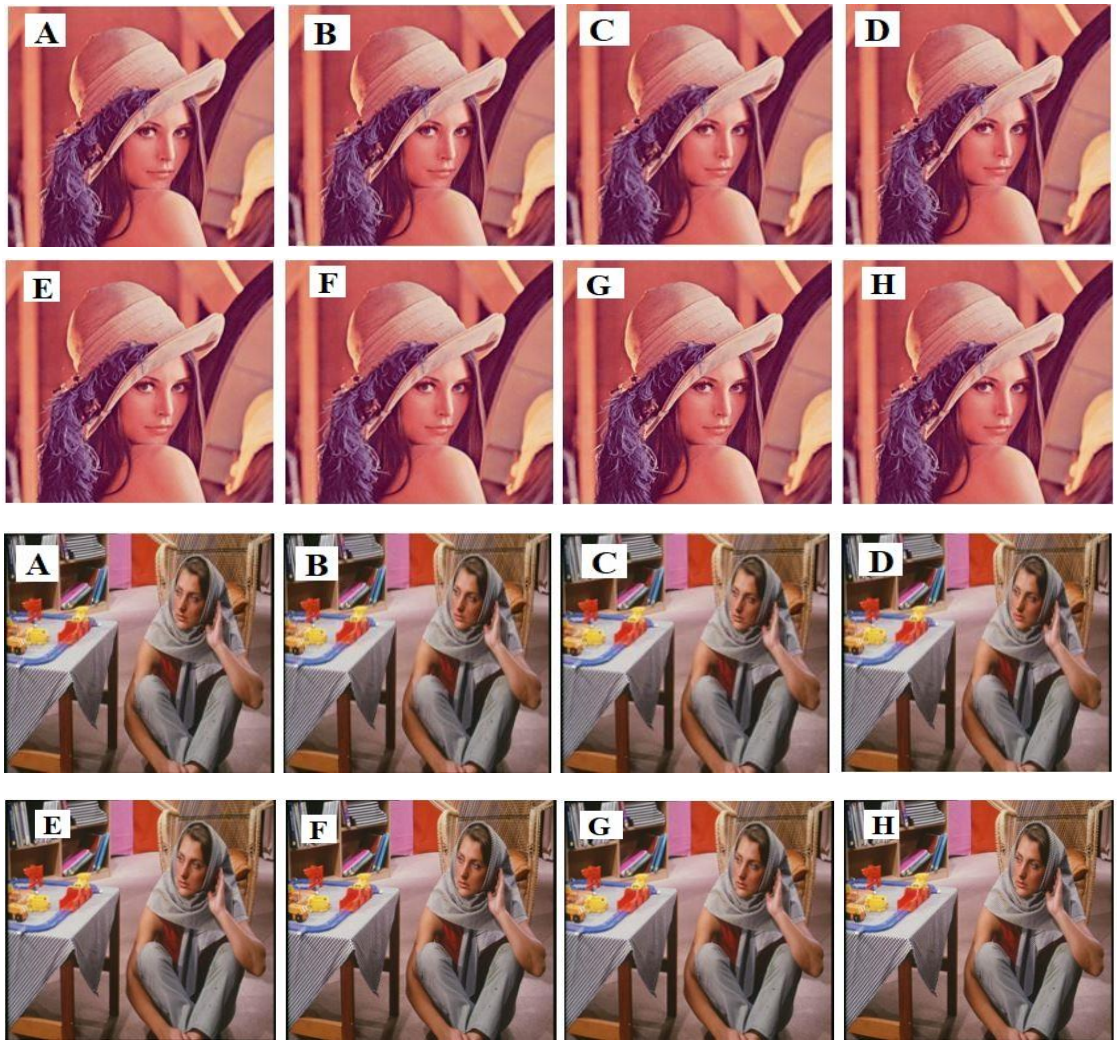


***Figure 11:** (A)-(D) are the decrypted images after adding Speckle Noise with intensities of 0.000001, 0.000002, 0.000003, and 0.000004, and (E)-(H) are the decrypted images after adding Salt and Pepper Noise with intensities of 0.00001, 0.00003, 0.0005, and 0.0007, respectively.*

5.7. Occlusion attack analysis

The Occlusion attack aims to distort image data by blocking or cropping various regions of the encrypted image, which has a negative impact on the decryption process and may alter the image content in certain algorithms [33]. To test the algorithm's resistance to Occlusion attacks, it was assumed that Lena and Barbara's 512×512 images were subjected to an Occlusion attack with varying intensity and sparse areas, and the encrypted images affected by the attack were used in the decryption process. Figure (12) depicts the effect of the attack on the decrypted image. Despite the severity of the attack, the image is still comprehensible to the observer, indicating that the encrypted image is trustworthy and able to thwart the Occlusion attack.

Ali. A. Abdul-Kareem, Waleed A. M. Al-Jawher. (2022). Uruk 4D Discrete Chaotic Map for Secure Communication Application. Journal Port Science Research, 5(3), 131–142. https://doi.org/10.36371/port.2022.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

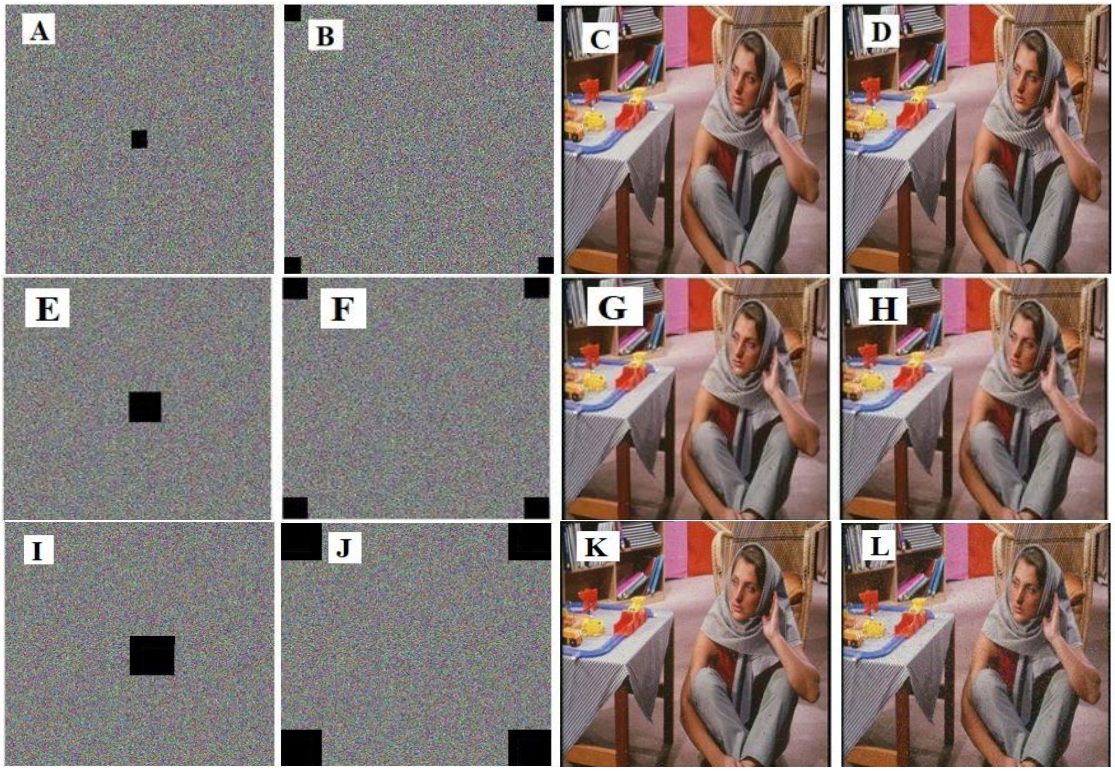


Figure 12: *(A, B) encrypted images with loss data sizes 16×16 pixel per square, (C, D) are the decrypted images with PSNR 31.6279 and 31.5396, respectively, (E, F) are encrypted images with loss data sizes 32×32 pixel per square, (G, H) are the decrypted images with PSNR 32.5835 and 26.6209, respectively, (I, J) encrypted images with loss data sizes 64×64 pixel per square, (K, L) are the decrypted images with PSNR 26.6562 and 20.6605, respectively*

6. RESULTS AND METHODOLOGY DISCUSSION

The analysis and simulations were conducted under identical conditions on the same machine, Lenovo Windows 10 Pro; Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.60 GHz; RAM: 16GB. The chaotic properties tests revealed that the proposed system has highly chaotic dynamics and a high sensitivity to initial conditions, as well as long-range chaotic strings with low computational complexity. Information entropy test and differential attack results for encoded images are very close to the optimal value. In contrast, comparisons with other cipher algorithms based on chaotic systems revealed that the proposed encryption algorithm is extremely competitive and vastly superior. The proposed image encryption system is therefore highly secure and reliable for the majority of communications and data security requirements.

7. CONCLUSION

This paper proposes the URUK discrete four-dimensional chaotic map for the generation of high-quality, long-range chaotic sequences. Analyzing the principal characteristics of phase images, the Lyapunov Exponent tests, 0-1 tests, and the NSIT tests revealed that the complex dynamics of the proposed system are highly chaotic, independent, and computationally simple. Moreover, the used security measurements and computer simulation confirmed that Uruk secret keys are able to provide better protection against statistical, differential, and brute force attacks, where the algorithm based on Uruk Secret Keys has proven to have strong encryption procedures and high computational speed, and can overcome common weaknesses found in encryption algorithms based on other chaotic systems.

REFERENCES

[1] Wang, X., Feng, Y., & Chen, Y. (2022). A New Four-Dimensional Chaotic System and its Circuit Implementation. Frontiers in Physics, 376 .https://doi.org/10.3389/fphy.2022.906138

[2] Abdullah, Hamsa A.; Abdullah, Hikmat N.; Mahmoud Al-Jawher, Waleed A. (2019). A hybrid chaotic map for communication security applications. International Journal of Communication Systems, (), e4236–. https://doi:10.1002/dac.4236

[3] J. Wen, Y. Feng, X. Tao and Y. Cao, "Dynamical Analysis of a New Chaotic System: Hidden Attractor, Coexisting-Attractors, Offset Boosting, and DSP Realization," in IEEE Access, vol. 9, pp. 167920-167927. https://doi:10.1109/ACCESS.2021.3136249

[4] Ali Akram Abdul-Kareem, Prof. Waleed Ameen Mahmoud Al-Jawher(2022) "WAM 3D Discrete Chaotic Map for Secure Communication Applications" Proceeding of 3rd International Conference on Optics, Photonics and Lasers, 20-21 September, 2022.

[5] J. Wen, Y. Feng, X. Tao and Y. Cao, (2021). Dynamical Analysis of a New Chaotic System: Hidden Attractor, Coexisting-Attractors, Offset Boosting, and DSP Realization, in IEEE Access, vol. 9, pp. 167920-167927, https://doi:10.1109/ACCESS.2021.3136249

[6] Dong, C. (2022). Dynamics, periodic orbit analysis, and circuit implementation of a new chaotic system with hidden attractor. Fractal and Fractional, 6(4), 190 .https://doi.org/10.3390/fractalfract6040190

[7] Rahman, Z. A. S., Jasim, B. H., Al-Yasir, Y. I., Abd-Alhameed, R. A., & Alhasnawi, B. N. (2021). A new no equilibrium fractional order chaotic system, dynamical investigation, synchronization, and its digital implementation. Inventions, 6(3), 49. https://doi.org/10.3390/inventions6030049

[8] Chenguang Ma; Jun Mou; Li Xiong; Santo Banerjee; Tianming Liu; Xintong Han; (2021). Dynamical analysis of a new chaotic system: asymmetric multi-stability, offset boosting control and circuit realization. Nonlinear Dynamics. https://doi:10.1007/s11071-021-06276-8

[9] Chuanfu Wang;Yi Di;Jianyu Tang;Jing Shuai;Yuchen Zhang;Qi Lu; (2021). The Dynamic Analysis of a Novel Reconfigurable Cubic Chaotic Map and Its Application in Finite Field. Symmetry, (), –. https://doi:10.3390/sym13081420

[10] Skokos, C., Gottwald, G. A., & Laskar, J. (Eds.). (2016). Chaos Detection and Predictability. Lecture Notes in Physics. https://doi:10.1007/978-3-662-48410-4

[11] Gottwald, G. A., & Melbourne, I. (2004). A new test for chaos in deterministic systems. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 460(2042), 603–611. https://doi:10.1098/rspa.2003.1183

[12] Gottwald, Georg A.; Melbourne, Ian (2009). On the Implementation of the 0–1 Test for Chaos. SIAM Journal on Applied Dynamical Systems, 8(1), 129–145. https://doi:10.1137/080718851

[13] 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 Dyn 94, 723–744. https://doi.org/10.1007/s11071-018-4390-z

[14] Bassham, L., Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Leigh, S., Levenson, M., Vangel, M., Heckert, N. and Banks, D. (2010), A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

[15] Lin Teng; Xingyuan Wang; Feifei Yang; Yongjin Xian; (2021). Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. Nonlinear Dynamics, (), –. https://doi:10.1007/s11071-021-06663-1

[16] Duzhong Zhang; Lexing Chen; Taiyong Li; (2021). Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation. Entropy, (), –. https://doi:10.3390/e23030361

[17] Pourjabbar Kari, Ahmad; Habibizad Navin, Ahmad; Bidgoli, Amir Massoud; Mirnia, Mirkamal (2020). A new image encryption scheme based on hybrid chaotic maps. Multimedia Tools and Applications, (), –. https://doi:10.1007/s11042-020-09648-1

[18] Belqassim Bouteghrine;Camel Tanougast;Said Sadoudi; (2021). Novel image encryption algorithm based on new 3-d chaos map. Multimedia Tools and Applications, (), –. https://doi:10.1007/s11042-021-10773-8

[19] Hanif, Muhammad; Naqvi, Rizwan Ali; Abbas, Sagheer; Khan, Muhammad Adnan; Iqbal, Nadeem (2020). A Novel and Efficient 3D Multiple Images Encryption Scheme Based on Chaotic Systems and Swapping Operations. IEEE Access, (), 1–1. https://doi:10.1109/access.2020.3004536

[20] Ali Momeni Asl;Ali Broumandnia;Seyed Javad Mirabedini; (2021). Scale Invariant Digital Color Image Encryption Using a 3D Modular Chaotic Map. IEEE Access, () –. https://doi:10.1109/access.2021.3096224

[21] Bashir, Zia; Iqbal, Nadeem; Hanif, Muhammad (2020). A novel gray scale image encryption scheme based on pixels' swapping operations. Multimedia Tools and Applications, (), –. https://doi:10.1007/s11042-020-09695-8

[22] Xiaoliang Qian;Qi Yang;Qingbo Li;Qian Liu;Yuanyuan Wu;Wei Wang; (2021). A Novel Color Image Encryption Algorithm Based on Three-Dimensional Chaotic Maps and Reconstruction Techniques. IEEE Access, (), –. https://doi:10.1109/access.2021.3073514

[23] Shannon, C. E. (1948). A Mathematical Theory of Communication. Bell System Technical Journal, 27(3), 379–423. https://doi:10.1002/j.1538-7305.1948.tb01338.x

[24] Khan, L. S., Hazzazi, M. M., Khan, M., & Jamal, S. S. (2021). A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes. Chinese Journal of Physics, vol. 72, pp. 558–574. https://doi:10.1016/j.cjph.2021.03.02910.1016/j.cjph.2021.03.029

[25] Al-Maadeed, T. A., Hussain, I., Anees, A., & Mustafa, M. T. (2021) A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes. Multimedia Tools and Applications. Vol. 80, pp. 24801–24822. https://doi:10.1007/s11042-021-10695-5

[26] Teng, L., Wang, X., Yang, F., & Xian, Y. (2021). Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. Nonlinear Dynamics, vol. 105 (2), pp. 1859–1876. https://doi:10.1007/s11071-021-06663-1

[27] 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, vol. 9, pp. 61334–61345. https://doi:10.1109/access.2021.3073514

[28] Khalil, N., Sarhan, A., & Alshewimy, M. A. M. (2021). An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. Optics & Laser Technology, 143, 107326. https://doi:10.1016/j.optlastec.2021.1073

[29] Yaghouti Niyat, Abolfazl; Moattar, Mohammad Hossein (2019). Color image encryption based on hybrid chaotic system and DNA sequences. Multimedia Tools and Applications, (), –. https://doi:10.1007/s11042-019-08247-z

[30] Fawad Masood; Maha Driss; Wadii Boulila; Jawad Ahmad; Sadaqat Ur Rehman; Sana Ullah Jan; Abdullah Qayyum; William J. Buchanan; (2021). A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations. Wireless Personal Communications, (), –. https://doi:10.1007/s11277-021-08584-z

[31] Joshi, Anand B.; Kumar, Dhanesh; Mishra, D.C.; Guleria, Vandana (2020). Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map. Journal of Modern Optics, (), 1–17. https://doi:10.1080/09500340.2020.1789233

[32] Liu, Hui; Zhao, Bo; Huang, Linquan (2019). A novel quantum image encryption algorithm based on crossover operation and mutation operation. Multimedia Tools and Applications, (), –. https://doi:10.1007/s11042-019-7186-3

[33] Luo, Y., Liang, Y., Zhang, S., Liu, J., & Wang, F. (2022). An image encryption scheme based on block compressed sensing and Chen system. https://doi.org/10.21203/rs.3.rs-1604114/v1