

# Image scrambler based on novel 4-D hyperchaotic system and magic square with fast Walsh–Hadamard transform

Hayder Kadhim Zghair, Hussein Ali Ismael, Ameer Al-Haq Al-Shamery

Department of Software, Information Technology, University of Babylon, Babylon, Iraq

## Article Info

### Article history:

Received Jul 1, 2022

Revised Aug 18, 2022

Accepted Sep 2, 2022

### Keywords:

4-D hyperchaotic system

Fractional dimension

Image encryption

Lyapunov exponent

SDIC

Waveform analysis

## ABSTRACT

A novel 4-D hyperchaotic system that have seven positive parameters in third order with thirteen terms is proposed, in this paper, the proposed chaotic behavior is proved by analysis of the Lyapunov's exponent, fractional dimension, zero-one test, sensitivity dependent on initial condition (SDIC), phase portraits, and waveform analysis, this study offers an innovative designed image encryption algorithm depending on a 4-D chaotic system using fast discrete Walsh-Hadamard transform and magic matrix that is both effective and simple for image encryption and gives it a higher level of security. This new 4-D hyperchaotic system is used to produce a random key in this algorithm. The implemented and simulated results using mathematica programs and MATLAB programs were supplied qualitatively and in figures. The proposed system is hyperchaotic, according to testing results, because it possesses two Lyapunov positive exponents.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Hayder Kadhim Zghair

Department of Software, Information Technology, University of Babylon

Babylon, Iraq

Email: hyderkkk@uobabylon.edu.iq

## 1. INTRODUCTION

Data security for multimedia is a significant concern in advanced open communication systems that are vulnerable to numerous types of attacks. Encryption is the primary mechanism for achieving this level of security. When compared to other types of multimedia files (like image or speech). The development of novel image encryption techniques that are both fast and secure has piqued the interest of academics working in the multimedia security field [1]–[3]. Hua and Zhou [4] proposed sine-logistic (SMLA-2D) module and designed ciphered image based on (SMLA-2D) to give a high level of security and improved ability to resist different attacks. The work in [5] suggested a new ciphered image to give this scheme more secure and safer, a researcher found the experimental results for security are very good for the suggested algorithm. Wang *et al.* [6] approved high security to ciphered images based on multi-chaos and coupling modules for improved ability of the ciphered image against several attacks. Song *et al.* [7] suggested a new spatial-temporal chaotic system that is based on spatial spread, local-nonlinear map, and then modular by coupled map lattices (CML) as a secure key for encryption image. This work is provided mechanism for diffusion and confusion rely on these chaotic maps by using XOR operation itself pixels of image to achieve diffusion and using secure key that generated from chaotic map to achieve confusion. Belazi *et al.* [8] proposed new image encryption technique based on chaotic maps and network of permutation\_substitution (SP). This study consists of four stages include diffusion achieved by new chaotic map, substitution achieved by s-boxes operation, diffusion achieved by new logistic map, and permutation operation to encrypt image. Chen *et al.* [9] proposed new 3D cat chaotic map for real time encryption. In this work, 3D Cat map used to shuffle the pixels of image and confused the relationship between original image and encryption image by used another chaotic map to increase the security. Liao *et al.* [10] suggested new encryption image

approach based on deoxyribonucleic acid (DNA) technique, SHA-256, and chaotic map. This study, used these techniques to generate secure key to encrypt image.

Chaos is a complex and random dynamical phenomenon in nonlinear systems. It is widely applied in information technology, electronic engineering, and various other fields, due to its boundedness initial value sensitivity, and inherent randomness. Researchers start to discover chaotic have more complex dynamical behaviors to make chaotic information encryption and chaotic secure communication more secure [11]–[14]. Zhou *et al.* [15] designed a smooth quadratic 4-D autonomous hyperchaotic system having complex dynamical behavior, then analyzed Hopf bifurcation, Pitchfork bifurcation, the stability of the system and other dynamical problems by applying the central manifold theory and bifurcation theory. Li *et al.* [16] suggested the presence of zero-Hopf bifurcation by using the averaging theory and also proposed aperiodic for the proven Chua system solutions used the same theoretical. Jendoubi [17] improved the presence of aperiodic solution for delayed non-autonomous non-densely partial differential equations. The work in [18] approved zero-Hopf bifurcation of the 4-D system by using averaging theory. Huang *et al.* [19] suggested a 4-D chaotic system depending on Sprott's chaotic system. This paper proposes an improved image encryption strategy based on a 4-D hyperchaotic system with a five-term cross-product and seven positive parameters to produce the highest randomness based on a strong chaotic sequence with dynamic complexity when compared to fast Walsh–Hadamard transform (FWHT) employing magic squares and this system has proposed to give a high level of security compared to other methods. The following is how this article is organized: formulation of the novel 4-D system and description of chaos dynamical behavior, image encryption/decryption algorithm, security analysis, as well as a comparison of the suggested scheme, finally, there is a conclusion.

## 2. THE PROPOSED METHOD

This section includes i) demand formulation of a novel 4-d chaotic system, ii) analysis of chaos system, and iii) proposed image encryption.

### 2.1. Demand formulation of a novel 4-D hyperchaotic system

The proposed novel 4-D consists of thirteen terms with seven positive parameters in a third-order autonomous hyperchaotic system. It creates a new system by performing multiple experiments to determine the system's initial conditions ( $x(0), y(0)$  and  $z(0)$ ) and parameters ( $\sigma, \eta, \Omega, \mu, \beta, \mathcal{U}$  and  $\alpha$ ). The proposed novel 4-D was expressed as follows.

$$\frac{dx}{dt} = -\sigma yz - \beta x - \eta w. \quad (1)$$

$$\frac{dy}{dt} = \Omega x - x z w - y \quad (2)$$

$$\frac{dz}{dt} = x y w - \mathcal{U} z - x w - \mu x \quad (3)$$

$$\frac{dw}{dt} = \sigma xy - y z - w \quad (4)$$

Wherever  $(x, y, z, w)^T \in R^4$  also,  $\sigma, \eta, \Omega, \mu, \beta, \mathcal{U}$  and  $\alpha$  are positive system parameters. The 4-D system (1) generated a strange attractor and chaotic, while chaos parameter values are selected as follows:  $\sigma = 28, \eta = 2, \Omega = 25, \beta = 20, \mathcal{U} = 2.5, \mu = 5$  and  $\alpha = 26$  while the initial conditions are as follows:  $x(0) = 0.5, y(0) = 4, z(0) = 2.6$ , and  $w(0) = 3$  system of forms (1) Figures 1(a)-(d) show the strange attractor for a 4-D system in 3-D projection on  $(x, y, w), (x, y, z), (w, y, z), (z, w, x)$  space, respectively. Figures 2(a)-(c) show a chaotic portrait in 2-D projection on  $(x, z), (x, y)$ , and  $(w, x)$  space respectively.

### 2.2. Analysis some chaotic properties 4D

- Symmetry: the system (1) is symmetric w.r.t  $w$ - axis because the 4-D system is invariant under the coordinate transformation:  $(x, y, z, w) \rightarrow (-x, -y, -z, w)$ , hence the 4-D hyperchaotic (1) has a symmetric oscillation.
- Zero-one test: in deterministic dynamic systems, zero-one distinguishes between nonchaotic, and chaotic dynamics [20]. The K values acquired from the system (1) in which variables  $(x, y, z, \text{ and } w)$  are accomplished are as follows:  $k_x = 0.9366, k_y = 0.99593, k_z = 0.966124, k_w = 0.9614$ , we can prove that system (1) is chaotic because all K values have been determined to be close to one.
- The Lyapunov exponent by Alan Wolf [10] which was evaluated using MATLAB programming after 10,000 iterations with step size 0.05 for the system (1) are:  $L_1 = 2.1295, L_2 = 0.4467, L_3 = -4.9358$ , and  $L_4 = -22.0229$ , because the biggest  $L_1 > 0$ . The chaotic properties of the system (1) can be proved, the system also is hyperchaotic because the  $L_1$ , and  $L_2 > 0$  and reminder  $L_3$ , and  $L_4 < 0$ .

- The  $\mathcal{K}$ aplan-Yorke dimension  $\mathfrak{E}_{KY}$  [21] which is determined through Lyapunov exponents for system (1) where  $\mathfrak{E}_{KY}$  can be form as:

$$\mathfrak{E}_{KY} = j + \frac{1}{|L_{j+1}|} \sum_{i=1}^j L_i \text{ By arranging } L_1 > L_2 > L_3 > L_4 = 2 + \frac{2.1295+0.4467}{4.9358} = 2.52184 \quad (5)$$

where  $\sum_{i=1}^j L_i > 0$  and  $\sum_{i=1}^{j+1} L_i < 0$ . Hence  $\mathfrak{E}_{KY}$  hence the Lyapunov dimension is fractional as a result of this, because of its fractal character, the system (1) exhibits non-periodic orbits. As demonstrated in Figure 2, numerical simulation can be used to obtain the chaotic attractors of the system (1). Show the strange attractor for the 4-D system in 2-D projection on (x, z), (x, y), and (w, x) space respectively. Table 1 compares the proposed system (1) in terms of Lyapunov exponents to those found in the literature [15], [16], [19]. As can be observed the two positive Lyapunov exponents for the proposed system. It means that the hyperchaotic properties of the system (1) are more apparent and the system's dynamic characteristics are more difficult to predict (KEY). The following generates sequence keys with size (65,536) by using a novel 4-D hyperchaotic system to initialize three initial conditions  $(x_0, y_0, z_0)$  in addition to the seven secrets parameters  $\sigma = 28, \eta = 2, \Omega = 25, \beta = 20, \omega = 2.5, \mu = 5$  and  $\alpha = 26$  and of the system (1) to get a hyperchaotic sequences  $\{(y_n, x_n, z_n, w_n); \text{ where } n = 1, 2, \dots, 65536\}$  of variables for 4-D system.

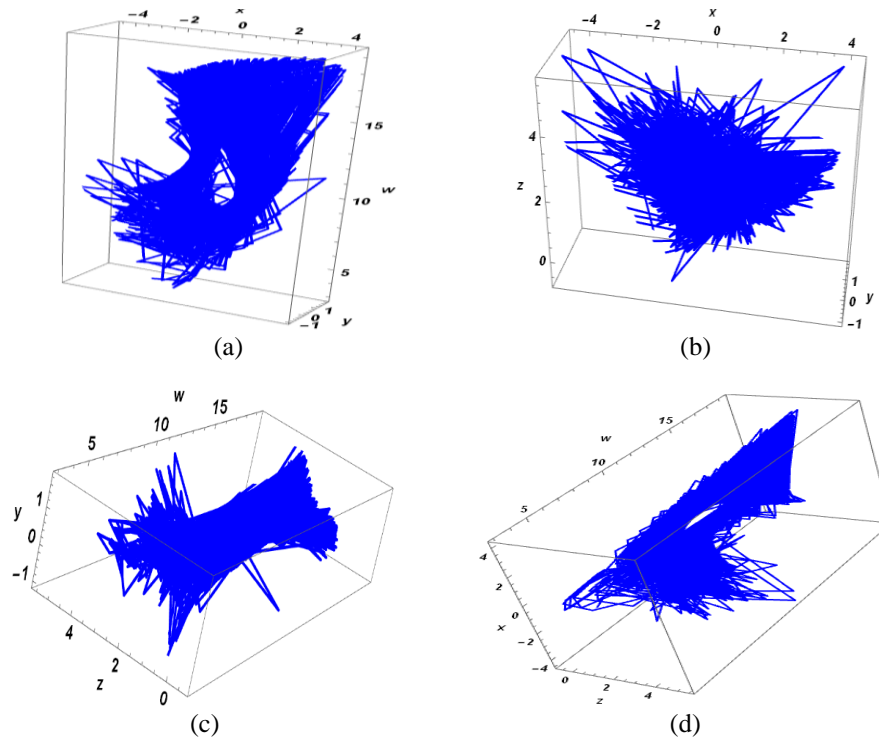


Figure 1. Chaotic portrait in 3-D projection in (a) (x, y, w), (b) (x, y, z), (c) (w, y, z), and (d) (z, w, x) space

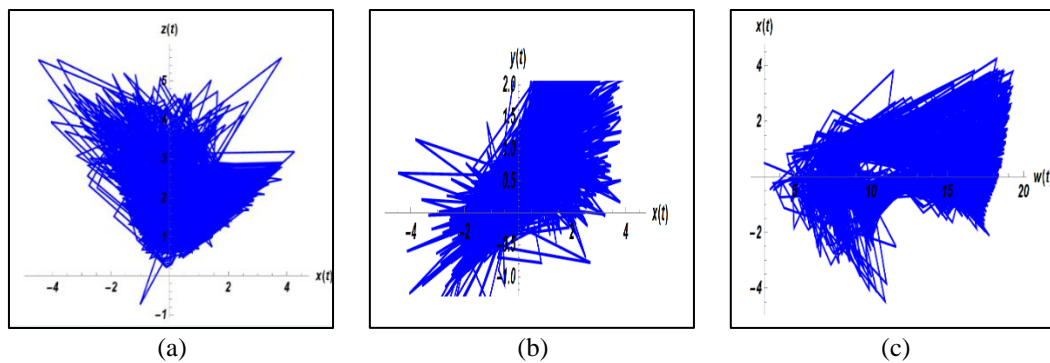


Figure 2. Chaotic portrait in 2-D projection on (a) (x, z) space, (b) (x, y) space, and (c) (w, x) space

Table 1. Description six chaotic systems: parameter and Lyapunov exponents

Reference	Parameter	Lyapunov Exponent (LEs)
[19]	a=6, b=11, c=5	One positive Lyapunov Exponent
[15]	b=3.9, c=3, a=2, d=1	One positive Lyapunov Exponent
[18]	b = 30, c = 4, d = 0.2, e = -0.1, k = 4	Two positive Lyapunov Exponent
Our system	$\sigma = 28, \eta = 2, \Omega = 25, \beta = 20, \omega = 2.5, \mu = 5$ and $\alpha = 26$	Large Two positive Lyapunov Exponent

- Waveform analysis: proved that the waveforms are aperiodic, and waveform's time domain has noncyclical properties [11], [12]. Figure 3(a) shown noncyclical properties of the time domain against state variable x, Figure 3(b) shown noncyclical properties of the time domain against state variable w and Figure 3(c) shown noncyclical properties of the time domain against state variable y for the proposed 4-D chaotic system.

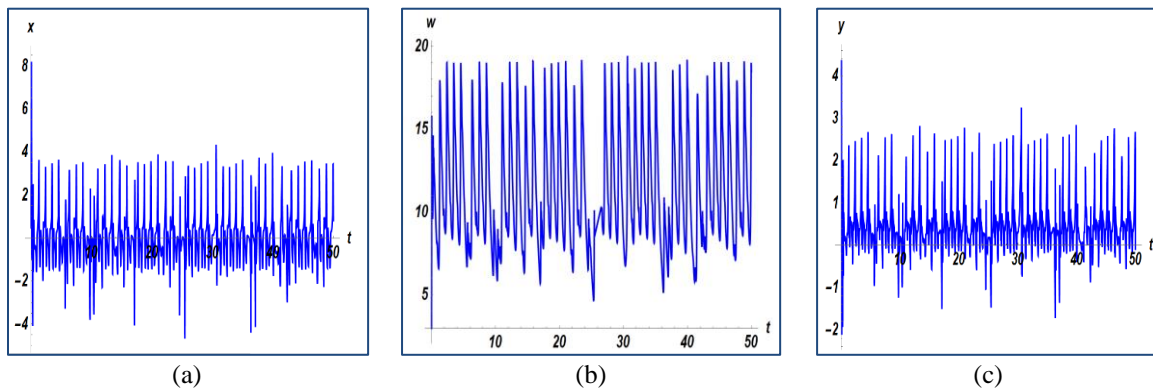


Figure 3. Time-domain waveform for the 4-D (a) time against x(t), (b) time against w(t), and (c) time against y(t)

**2.3. Proposed image encryption system**

The proposed image encryption scheme uses two techniques include the 4-D chaotic system and a magic matrix with FHWT transformation to generate secure keys that use to permute and encryption an image. Where key x that used to permute the magic array. The key w used to encryption. Figure 4 show the chaotic encryption system of the proposed image algorithm diagram.

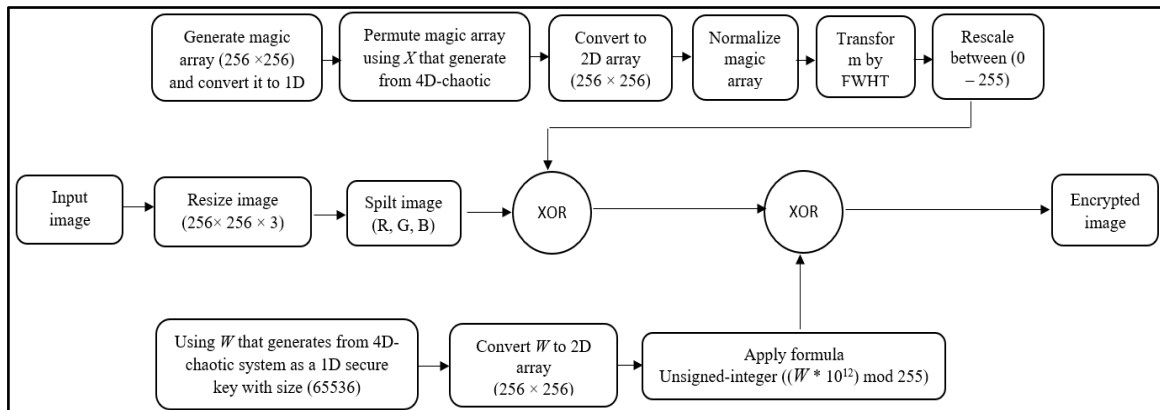


Figure 4. The chaotic encryption system of the proposed image algorithm diagram

**3. ENCRYPTION ALGORITHM**

When the encrypted image is received by the recipient. To begin, the receiver and transmitter must share the eleven secret keys to de-encrypted the encrypted image. The following are the eleven secret keys.  $\sigma, \eta, \Omega, \beta, \omega, \mu$  and  $\alpha$  system parameter values in addition to the initial conditions are  $x(0), y(0), z(0),$  and  $w(0)$ , secondly, by using the same proposed algorithms, starting with four initial

conditions  $(x_0, y_0, z_0, w_0)$  in addition to the seven secrets parameters  $\sigma, \eta, \Omega, \beta, \omega, \mu$  and  $\alpha$  to get the same secret key from the system (1) that the receivers use by applying the same proposed algorithms. Apply the eXclusive OR (XOR) operation between the encryption result and rescale intensity magic and so on, until transformed back to the original image. A magic square is a square matrix having arranged and integer values, with conditions that the sum of numbers in each row, each column, and the main diagonals are the same [22].

```

Input: image
Output: Encrypted image, keys include parameters and initial values of 4D chaotic map
Begin:
1: Read the original image and resize it to (256*256*3).
2: X, Y, Z, W: = Generate sequence keys with size (65536) by using a novel 4-D chaotic
   system.
3: Magic: = magic array (256*256).
4: Convert Magic to 1D array
5: Permutation of Magic using key X
6: Convert the previous result of Magic to a 2D array
7: Intensity_Magic: = normalize Magic between the minimum and maximum value in Magic
8: Trans_Intensity_Magic: = transform Intensity_Magic by FWHT transformation
9: Rescale_Intensity_Magic: = Rescale for Trans_Intensity Magic between (0 and 255)
10: W: = unsigned-integer ((W * 1012) mod 255)
11: W: = convert key W to 2D array
12: For I in three channels of image do:
    i. Permute Chi: = permutation Chi using key W
    ii. Between Permute Chi and Rescale Intensity Magic, perform the XOR operation.
    iii. Between the previous result and key W, perform the XOR operation
13: End for
14: Combine the three channels into an encrypted image
15: Send keys that include parameters and initial values to the sender by Diffie-Hellman
    (DH).
16: Send the encryption image to the receiver side.
End.

```

#### 4. RESULTS AND DISCUSSION

In this paper, the suggested algorithm has been used for the analysis of several images. The image that has been subjected to this test has a size of 256\*256 pixels although this algorithm can be used for images having a completely different size. The suggested algorithm will be proved for statistical analysis and security, and its effectiveness will be determined. The secret key of the encryption algorithm might be highly sensitive also to prevent brute force attacks and also to improve the security of these algorithms, to show the designed algorithm is highly resistant to statistical attack must be the length of keyspace greater than  $2^{128}$  [23]. Some analyses have been performed such as entropy, histogram, and correlation test for the encrypted image.

##### 4.1. Security analysis

To thwart assaults using brute force the secret keyspace must be sufficiently large [14], [23], [24]. The minimum size of the keyspace must be at least  $2^{128}$  bits. The chaotic system has seven parameters and four initial conditions. The precision of each parameter and initial condition equal to  $10^{-14}$ , so that the keyspace can be calculated as  $10^{154} \approx 2^{512}$ . that was large enough to thwart any assaults using brute force.

##### 4.2. Sensitivity test

An image-ciphered process must be quite sensitive to the encryption key [25]. MonaLisa has been selected as the original image to measure the sensitivity analysis. An encrypted image cannot be decrypted as long as there is a tiny change in the cipher key [26]. Cipher key  $y(0) = 4 \times 10^{-14}$  while keeping other parameters as they are. Comparison between the two encrypted images shows that even a very little difference of  $10^{-14}$ , attackers will not correctly decrypt the image. Figure 5(a) shown MonaLisa original image, Figure 5(b) shown ciphered image, Figure 5(c) shown deciphered image with the same parameters and initial condition and Figure 5(d) shown deciphered image with tiny change of initial condition.

##### 4.3. Statistical analysis test

Every statistical similarity or association between the original and ciphered images should be avoided to prevent attackers from knowing any information about the original image. Histogram analysis for this image will conclude the statistical properties of this image [27]. The statistical characteristics of an original and ciphered image must be entirely different to protect the information of the original image from attackers. Figure 6(a) shown the histogram test of MonaLisa original image and Figure 6(b) shown the histogram test of encrypted MonaLisa original image.

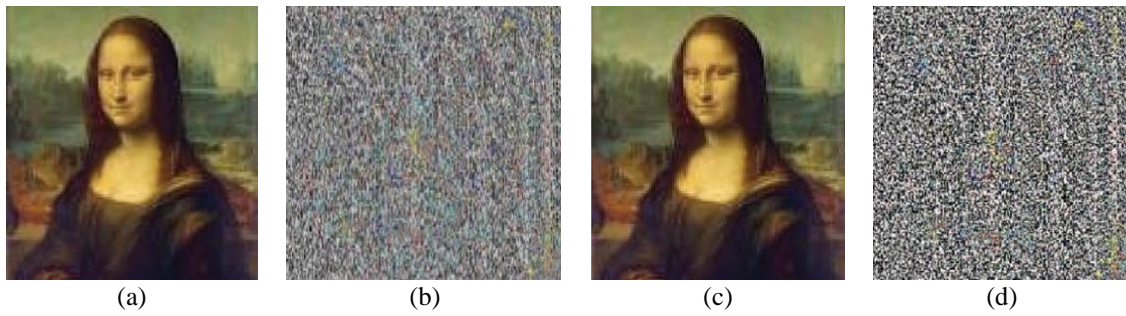


Figure 5. Results of sensitivity initial condition test (a) Monalisa original image, (b) ciphered Monalisa image, (c) where  $y(0)=4$  decrypted Monalisa image, and (d) where  $y(0)=4 \times 10^{-14}$  decrypted Monalisa image

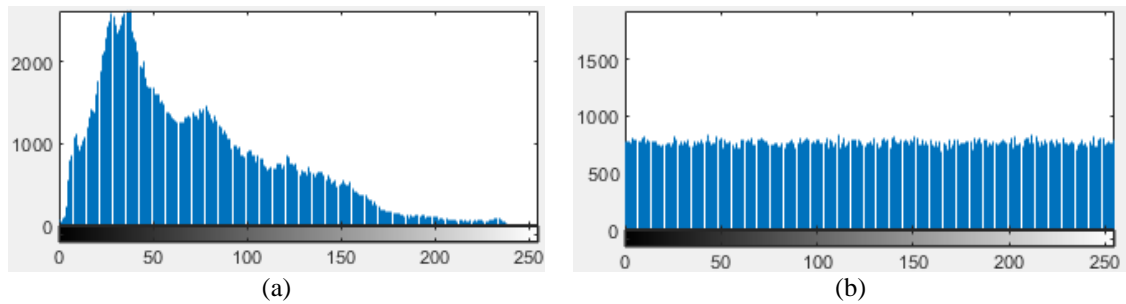


Figure 6. Results of histogram test (a) histogram Monalisa and (b) histogram Monalisa encrypted image

**4.4. Correlation coefficient test**

A high correlation of adjacent pixels is one of the main properties of any image correlation is defined as a measure of the extent of similarity between two pixels [28]. Figure 7 results of correlation test (Monalisa). To protect the values of the neighbor pixels from attackers any ciphered algorithm must be reduced the correlation between adjacent pixels [29]. The suggested scheme resists the statistical attackers by making the correlation closer to zero concerning the original image the correlation coefficient was calculated for both ciphered and original images of horizontally, diagonally, and vertically adjacent pixels. Table 2 describes the correlation test.

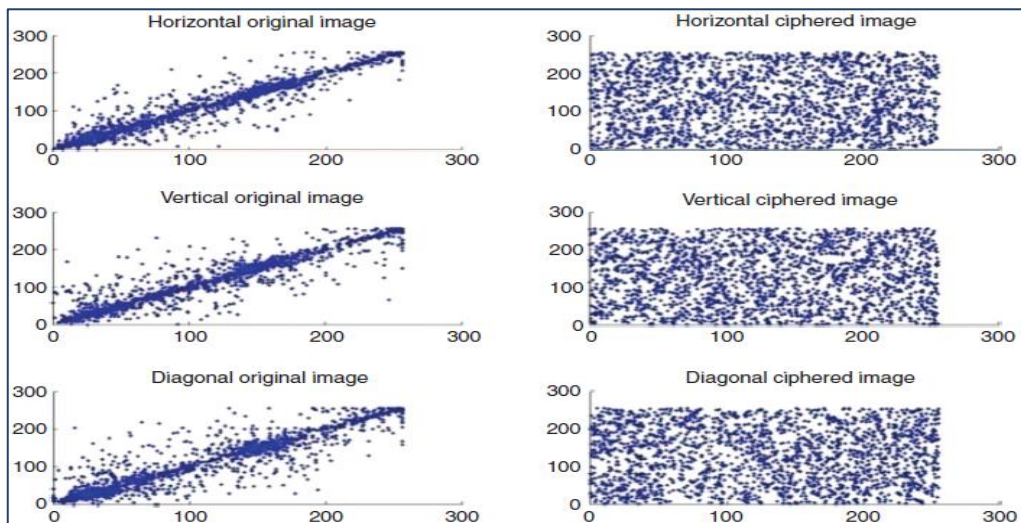


Figure 7. Results of the correlation test

Table 2. Description correlation test

Images	Parameter	Our Cipher	[1]	[5]	Directions
Baboon	0.9400	-0.0002	0.0056	-0.0005	Horizontal
	0.9448	-0.0006	0.0006	0.0088	Vertical
	0.9086	0.0002	-0.0001	-0.0007	Diagonal
Mona	0.7315	0.0002	0.0029	-0.0031	Horizontal
	0.998	0.0009	-0.0004	-0.0027	Vertical
	0.6411	0.0018	-0.0014	-0.0007	Diagonal
Rose	-0.0026	0.0001	0.0009	0.0033	Horizontal
	-0.0027	0.0020	0.0028	0.0092	Vertical
	-0.0001	0.0014	0.0027	0.0055	Diagonal

#### 4.5. Information entropy test

The most significant component of randomness or unpredictable behavior in information was entropy [30]. To prove that the proposed image encryption system is resistant to different attacks and highly secure have a range from (7.9990-7.9995). This indicates that the original image has a less degree of randomness than the ciphered image. Table 3 proves the security against different attacks was excellent.

Table 3. Comparison entropy test

Our	[6]	[4]	[7]	[8]	[9]	[10]
7.9995	7.9987	7.9982	7.9973	7.9977	7.9975	7.9973

#### 4.6. Differential attack

A perfect proposed image encryption system must possess the attribute the resist differentiation attacks [31]. Test of differential attacks consists of two encrypted original images having a tiny difference equal to 1 bit and the effect of this difference on the produced encrypted image was measured important measures used in this analysis include unified averaged changed intensity (UACI) and number of changing pixel rate (NPCR) [24]–[28]. Table 4 shows the UACI and NPCR for different images. The resulting values of UACI range between (33.3-33.345) and that of NPCR range between (99.5-99.6114) therefore our experiment results prove that this proposed algorithm was highly resistant to differential attacks.

Table 4. Comparison differential attack test

Our	[4]	[7]	[8]	[9]	[10]	Our
Mean UACI	99.609	99.584	99.617	99.602	99.608	99.611
Mean NPCR	33.4023	33.4937	33.4936	33.4076	33.6694	33.349

#### 4.7. Time performance

An important factor for analysis of the proposed algorithm was the speed utilized to assess the efficiency of the proposed image encryption system implemented in software MATLAB 2018b based on Xcx64 windows 10 using core™ i7 with RAM adopted is 4 GB. The Time performance in second of our proposed system equal to (0.821 sec) it is less than the system in [10]. Table 5 shows the time performance of the proposed scheme.

Table 5. Comparison Time performance

Image size	[10]	[9]	[8]	Our
256*256	6.01	< 0.4	0.095	0.82107

## 5. CONCLUSION

A novel 4-D hyperchaotic system that has seven positive parameters in third order with thirteen terms is proposed for generating a secure key to encrypt an image. It has been proved by the chaotic analysis is strong based on Lyapunov's exponent, fractional dimension, zero-one test, SDIC, phase portraits, and waveform analysis. This study offers an innovative designed image encryption algorithm depending on a 4-D chaotic system using fast discrete Walsh-Hadamard transform and magic matrix that is both simple and effective for image encryption and gives a higher level of security and hyperchaotic system. This system has proven to give a high level of security compared to other methods. As it produced an ideal encrypted image due to having a high level of entropy test up to (7.9995) as well as a low level of correlation test up to (0.0001). In addition,

having a high key space of up to ( $2^{512}$ ). But the performance of speed is (0.82107 s). According to previous results, conclude that a secure image encryption system is stronger than other systems that have been evaluated recently.

## REFERENCES





- [1] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the lss chaotic map and single S-Box," *IEEE Access*, vol. 8, pp. 25664–25678, Jun. 2020, doi: 10.1109/ACCESS.2020.2970806.
- [2] H. A. Ismael, A. A. Abdullah, and Z. A. Abod, "Enhancement of speech scrambles using DNA technique and chaotic maps over transformation domain," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 9, no. 2, pp. 510–523, Mar. 2021, doi: 10.21533/PEN.V9I2.1834.
- [3] Z. A. Abod, H. A. Ismael, and A. A. Abdullah, "Chaos-based speech steganography and quantum one time pad," *Journal of Engineering and Applied Science*, vol. 13, no. 3, pp. 739–745, Feb. 2018, doi: 10.36478/jeasci.2018.739.745.
- [4] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, Apr. 2016, doi: 10.1016/J.INS.2016.01.017.
- [5] X.-P. Zhang *et al.*, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *Chinese Physics*, vol. 27, no. 8, p. 080701, Aug. 2018, doi: 10.1088/1674-1056/27/8/080701.
- [6] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Scientific reports*, vol. 10, no. 1, pp. 1–15, Jun. 2020, doi: 10.1038/s41598-020-66486-9.
- [7] C. Y. Song, Y. L. Qiao, and X. Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3329–3334, Sep. 2013, doi: 10.1016/J.IJLEO.2012.11.002.
- [8] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, Nov. 2016, doi: 10.1016/J.SIGPRO.2016.03.021.
- [9] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004, doi: 10.1016/J.CHAOS.2003.12.022.
- [10] Aqeel-ur-Rehman, X. Liao, A. Kulsoom, and S. Ullah, "A modified (dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps," *Multimedia Tools and Applications*, vol. 75, no. 18, pp. 11241–11266, Aug. 2015, doi: 10.1007/S11042-015-2851-7.
- [11] M. A. A. K. AL-Yaseen and H. K. Zghair, "Some chaotic properties of 2-D rational discrete map," *Journal of Interdisciplinary Mathematics*, vol. 24, no. 5, pp. 1127–1131, Oct. 2020, doi: 10.1080/09720502.2020.1790744.
- [12] O. M. Al-Hazaimah, A. A. Abu-Ein, K. M. Nahar, and I. S. Al-Qasrawi, "Chaotic elliptic map for speech encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 2, pp. 1103–1114, Feb. 2022, doi: 10.11591/IJEECS.V25.I2.PP1103-1114.
- [13] A. H. Khaleel and I. Q. Abduljaleel, "Secure image hiding in speech signal by steganography-mining and encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, pp. 1692–1703, Mar. 2021, doi: 10.11591/IJEECS.V21.I3.PP1692-1703.
- [14] O. M. Al-Hazaimah, "A new speech encryption algorithm based on dual shuffling Hénon chaotic map," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 3, pp. 2203–2210, Jun. 2021, doi: 10.11591/IJECE.V11I3.PP2203-2210.
- [15] L. Zhou, Z. Chen, J. Wang, and Q. Zhang, "Local bifurcation analysis and global dynamics estimation of a novel 4-dimensional hyperchaotic system," *International Journal of Bifurcation and Chaos*, vol. 27, no. 2, p. 1750021, Mar. 2017, doi: 10.1142/S0218127417500213.
- [16] J. Li, Y. Liu, and Z. Wei, "Zero-Hopf bifurcation and Hopf bifurcation for smooth Chua's system," *Advances in Difference Equations*, vol. 2018, no. 1, pp. 1–17, Dec. 2018, doi: 10.1186/S13662-018-1597-8/TABLES/1.
- [17] C. Jendoubi, "On the theory of periodic solution for some nonautonomous delayed partial differential equations," *Mathematical Methods in the Applied Sciences*, vol. 42, no. 18, pp. 6588–6606, Dec. 2019, doi: 10.1002/MMA.5763.
- [18] J. Yang, Z. Wei, and I. Moroz, "Periodic solutions for a four-dimensional hyperchaotic system," *Advances in Difference Equations*, vol. 2020, no. 1, pp. 1–9, May 2020, doi: 10.1186/S13662-020-02647-4.
- [19] L. Huang, Z. Zhang, J. Xiang, and S. Wang, "A new 4D chaotic system with two-wing, four-wing, and coexisting attractors and its circuit simulation," *Complexity*, vol. 2019, Oct. 2019, doi: 10.1155/2019/5803506.
- [20] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Bifurcation of novel seven-dimension hyper chaotic system," in *Journal of Physics: Conference Series*, vol. 1804, no. 1, p. 012051, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012051.
- [21] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Design and analytic of a novel seven-dimension hyper chaotic systems," *2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA)*, 2020, pp. 77–81, doi: 10.1109/IT-ELA50150.2020.9253077.
- [22] R. H. Al-Hashemy and S. A. Mehdi, "A new algorithm based on magic square and a novel chaotic system for image encryption," *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1202–1215, Jan. 2019, doi: 10.1515/JISYS-2018-0404.
- [23] A. A. Maryoosh, Z. S. Dhaif, and R. A. Mustafa, "Image confusion and diffusion based on multi-chaotic system and mix-column," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 4, pp. 2100–2109, Aug. 2021, doi: 10.11591/EEI.V10I4.2942.
- [24] S. F. Hamood, M. S. M. Rahim, and O. F. Mohammado, "Chaos image encryption methods: a survey study," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 1, pp. 99–104, Mar. 2017, doi: 10.11591/EEI.V6I1.599.
- [25] H. Kadhim Zghair, S. A. Mehdi, and S. B. Sadkhan, "Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system," in *Journal of Physics: Conference Series*, vol. 1804, no. 1, p. 012048, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012048.
- [26] S. B. Sadkhan and H. Ali, "A proposed speech scrambling based on hybrid chaotic key generators," in *Al-Sadiq International Conference on Multidisciplinary in IT and Communication Techniques Science and Applications, AIC-MITCSA 2016*, May. 2016, pp. 227–232, doi: 10.1109/AIC-MITCSA.2016.7759941.
- [27] A. Susanto *et al.*, "Triple layer image security using bit-shift, chaos, and stream encryption," *Bulletin of Electrical Engineering and Informatics* vol. 9, no. 3, pp. 980–987, Jun. 2020, doi: 10.11591/EEI.V9I3.2001.
- [28] H. A. H. A. Ismael and S. B. S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps," in *2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017*, Jul. 2017, pp. 132–137, doi: 10.1109/NTICT.2017.7976141.
- [29] O. Z. Akif, S. M. Ali, R. S. Ali, and A. K. Farhan, "A new pseudorandom bits generator based on a 2D-chaotic system and diffusion







- property,” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1580–1588, Jun. 2021, doi: 10.11591/EEI.V10I3.2610.
- [30] O. M. Al-hazaimeh, A. A. Abu-Ein, M. M. Al-Nawashi, and N. Y. Gharaibeh, “Chaotic based multimedia encryption: a survey for network and internet security,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 4, pp. 2151–2159, Aug. 2022, doi: 10.11591/EEI.V11I4.3520.
- [31] S. V. Kartalopoulos, “Differentiating data security and network security,” *2008 IEEE International Conference on Communications*, May 2008, pp. 1469–1473, doi: 10.1109/ICC.2008.284.

## BIOGRAPHIES OF AUTHORS







**Hayder Kadhim Zghair**     received bachelor degree in Mathematics from College of Education for Pure Sciences, Department of Mathematics, University of Babylon, Iraq in 2009. He received the master degree in Mathematics from College of Education for Pure Sciences, Department of Mathematics, University of Babylon, Iraq in 2012. He received the Master Ph.D, degree in Mathematics from College of Education, Department of Mathematics, Mustansiriyah University, Iraq in 2021. His research interests include chaotic systems, dynamical systems, topology, and encryption. He can be contacted at email: hyderkkk@uobabylon.edu.iq.



**Hussein Ali Ismael**     received Bachelor degree in Computer Science from College of Science, Department of Computer Science, University of Babylon, Iraq in 2010. He received the master degree in Computer Science from Faculty of Information Technology University of Babylon, Iraq in 2016. Currently He is Ph.D. Student Information Technology-Department of Software, Babylon University Babylon, Iraq. His research interests include AI and deep learning with medical healthcare. He can be contacted at email: husseinyessari@uobabylon.edu.iq.



**Ameer Al-Haq Al-Shamery**     received bachelor degree in Computer Science from College of Science, Department of Computer Science, University of Babylon, Iraq in 2011. He received the master degree in Computer Science from Faculty of Information Technology University of Babylon, Iraq in 2017. He received the Ph.D degree in Computer Science from Faculty of Information Technology, University of Babylon, Iraq in 2022. His research interests include AI and deep learning with business intelligence. He can be contacted at email: ameeralhaq@itnet.uobabylon.edu.iq.