

Analysis and description S-box generation for the AES algorithm-a new 3D hyperchaotic system

Hayder Kadhim Zghair¹, Mehdi Ebady Manaa², Safa Saad A. Al-Murieb¹,
Fryal Jassim Abd Al-Razaq¹

¹Department of Software, Information Technology, University of Babylon, Babylon, Iraq

²Department of Information Networks, Information Technology, University of Babylon, Babylon, Iraq

Article Info

Article history:

Received Sep 19, 2022

Revised Sep 30, 2022

Accepted Nov 2, 2022

Keywords:

3-D hyperchaotic system
AES algorithm
Fractional-Kaplien dimension
Lyapunov exponent
SDIC
Waveform analysis

ABSTRACT

In this paper, a description, and analysis of a novel 3-D dimension hyperchaotic system is implemented. The proposed system oscillation is two-order autonomous and consisted of a nine-term and symmetric oscillation w.r.t x-axis. It is proved analysis by Kaplan-York dimension, waveform analysis, phase portrait, and Lyapunov exponent. This work-study stability and equilibrium point and Routh stability criteria produced that the new system has one unstable point from the type saddle-focus point. One of the characteristics of the proposed system is hyperchaotic since this system has two Lyapunov large than zero. This system is applied to generate a chaotic matrix_{16*16} (S-box) based in advanced encryption standard (AES) algorithm for text encryption and gives a high level of security. In addition to the description, and analysis S-box. Therefore. the proposed algorithm is satisfied the high randomness of entropy value and passes the National Institute of Standards and Technology (NIST) parameters and another test. Mathematica and MATLAB programs simulated some results.

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

In the past few decades, researchers have studied chaotic systems, chaos theory, and applications based on chaos a focal study point on the 3-D chaotic systems since the discovery of the first chaotic attractor by Lorenz in 1963 [1]. In recent years several chaotic systems have been established including Chen and Ueta [2], Zghair *et al.* [3], Hajipour and Aminabadi [4], ElBeltagy *et al.* [5], and lu systems [6], also self-excited and hidden attractors are two recent categories of chaotic attractors, attraction has a basin that does not cross any tiny neighborhoods of an equilibrium point which is called a hidden attractor, in contrast to [7], an attraction basin which has crossed tiny neighborhoods of an equilibrium point which is called a self-excited attractor. Zhang *et al.* [8] worked on a novel 3D chaotic system by applying a nonlinear cross-product to the 2nd equation of the Rucklidge system they found that the worked system has extremely complex dynamical behaviors [8]. Lassoued and Boubaker [9] provides a general survey about newly designed chaotic and hyperchaotic systems, this involves an analysis of the dynamical behaviors of these complex systems Salih *et al.* [10] designed a new approach by using a 3D Logistic map as a proposed key through the replacement of the predetermined XOR operation in advanced encryption standard (AES) algorithms. Faghani *et al.* [11] designed a new 3D chaotic system depending on the basic formula of quadratic Jerk systems having terms, and other systems having a stable node equilibrium point. Patra and Banerjee [12] prove that 3D systems have attractors such as higher

dimension torus and hyperchaotic which cannot be seen in 2D. Abdullah and Abraham [13] try to improve the Rivest–Shamir–Adleman (RSA) algorithms by applying a 3D chaotic system with an experiment characteristic designed for this purpose. The new proposed system analysis and describes complex dynamical behaviors by proving the Lyapunov exponent spectrum, phase portraits, symmetric, dissipation, entropy, SDIC, and Routh stability criteria, and waveform analysis of the proposed system. This article introduced a novel suggestion for improving the security of AES as a chaotic secure communication algorithm. The improvement is driven by generating an XOR *matrix*_{16×16} S-box table form for the AES algorithm using the proposed system. This article's body is organized as follows: section 1, analysis and describes the mathematical modeling of chaos behavior, the stability and equilibrium of a new 3D proposed system, and introduced Kaplan-Yorke dimension, Lyapunov exponent and waveform test. Section 2 describe proposed metode. Section 3, the proposed system generated a chaotic XOR *matrix*_{16×16}. Section 4, security analysis Entropy and National Institute of Standards and Technology (NIST) test result and discussion. The conclusion is presented in the final section.

2. THE PROPOSED METHOD

In this part overview analysis and describes a new 3D proposed system behavior. Also, stability and equilibrium, Kaplan-Yorke dimension, Lyapunov exponent, and waveform test of a new 3D proposed system. Addition generated S-box based on 3D proposed system; i) analysis and describes new mathematical modeling of chaotic behavior and ii) the proposed system generated a chaotic XOR *matrix*_{16×16}.

2.1. Analysis and describes mathematical modeling of chaotic behavior

Considering the 3D hyperchaotic system the proposed system is two-order autonomous and consists of nine terms where xy, xz are the quadratic cross-product nonlinear term and it has two-term, one of them. sine and another cosine function, the proposed hyperchaotic 3D system is written as expressed:

$$\begin{aligned}\frac{dx}{dt} &= -\eta x - \sigma z^2 + \beta \cos(y) \\ \frac{dy}{dt} &= \rho \sin(x) - y - xz \\ \frac{dz}{dt} &= \omega y + \mu xy - \Omega z\end{aligned}\quad (1)$$

The proposed system has seven positive parameters $\beta, \sigma, \eta, \Omega, \rho, \omega$ and μ , and three initial conditions $(x(0), y(0), z(0))$, where $(x, y, z)^T \in R^3$, a strange attractor and hyperchaotic behaviors generated by the proposed system when $(\beta, \sigma, \eta, \Omega, \rho, \omega, \mu) = (1.5, 1.38, 11, 2.5, 30, 15, 5)$ and $(x(0), y(0), z(0)) = (3.6, 1, 2.6)$, therefore the keyspace for this system is very high and by the coordinate transformation: $(x, y, z) \rightarrow (x, -y, -z)$, the proposed 3D hyperchaotic system (1) is invariant. Therefore, 3D hyperchaotic system (1) is a symmetric oscillation w.r.t x-axis. Figure 1(a) phase partial for the proposed system in 2-D plan space (x,y), Figure 1(b) phase partial for the proposed system in 2-D plan space (x,z), Figure 1(c) phase partial for the proposed system in 2-D plan space (y,z), and Figure 1(d) attractors simulated in mathematica which display phase partial for the proposed system in 3-D (x,y,z) space.

2.1.1. Stability and equilibrium of a new 3D proposed system

By setting $\dot{x} = \dot{y} = \dot{z} = 0$, to solve the system (1):

$$\begin{aligned}0 &= -\eta x - \sigma z^2 + \beta \cos(y) \\ 0 &= \rho \sin(x) - y - xz \\ 0 &= \omega y + \mu xy - \Omega z\end{aligned}$$

We obtain by substitution $(\beta, \sigma, \eta, \Omega, \rho, \omega, \mu) = (1.5, 1.38, 11, 2.5, 30, 15, 5)$ one equilibrium point v (0.00012, 0.0037, 0.0223), the linearized for the proposed system (1) at v with Jacobian matrix is:

$$j = \begin{bmatrix} -\eta & -\sin(y) & -2z\sigma \\ -z + \rho\cos(x) & -1 & -x \\ y\mu & x\mu + \omega & -\Omega \end{bmatrix} = \begin{bmatrix} -11 & -0.00367 & -0.0615 \\ 29.9776 & -1 & -0.00012 \\ 0.0555 & 5.0018 & -2.5 \end{bmatrix}, \text{ let } |\lambda I - j| = 0$$

The eigenvalue of v is gained as $\lambda_1 = -3.34 - 6.91i$, $\lambda_2 = -3.34 + 6.91i$ and $\lambda_3 = 14.188$. The system at the point v is a saddle point, and the saddle-focus v has two dimensions stable manifold and a one-dimension unstable manifold, so this equilibrium point is unstable. Therefore, the characteristic equation is $-\lambda^3 + (-1 - \eta - \Omega)\lambda^2 + (-\eta - 2yz\mu\sigma + x(-x\mu - \omega) - \Omega - \eta\Omega - z\beta\sin(y) + \beta\rho\cos[x]\sin(y))\lambda +$

$2 y z \mu \sigma + x \eta (-x \mu - \omega) - 2 z^2 \sigma (-x \mu - \omega) - \eta \Omega + 2 z \rho \sigma (-x \mu - \omega) \cos(x) - xy\beta\mu \sin(y) - z\beta\Omega \sin(y) + \beta\rho\Omega \cos(x) \sin(y) = 0$ which implies that:

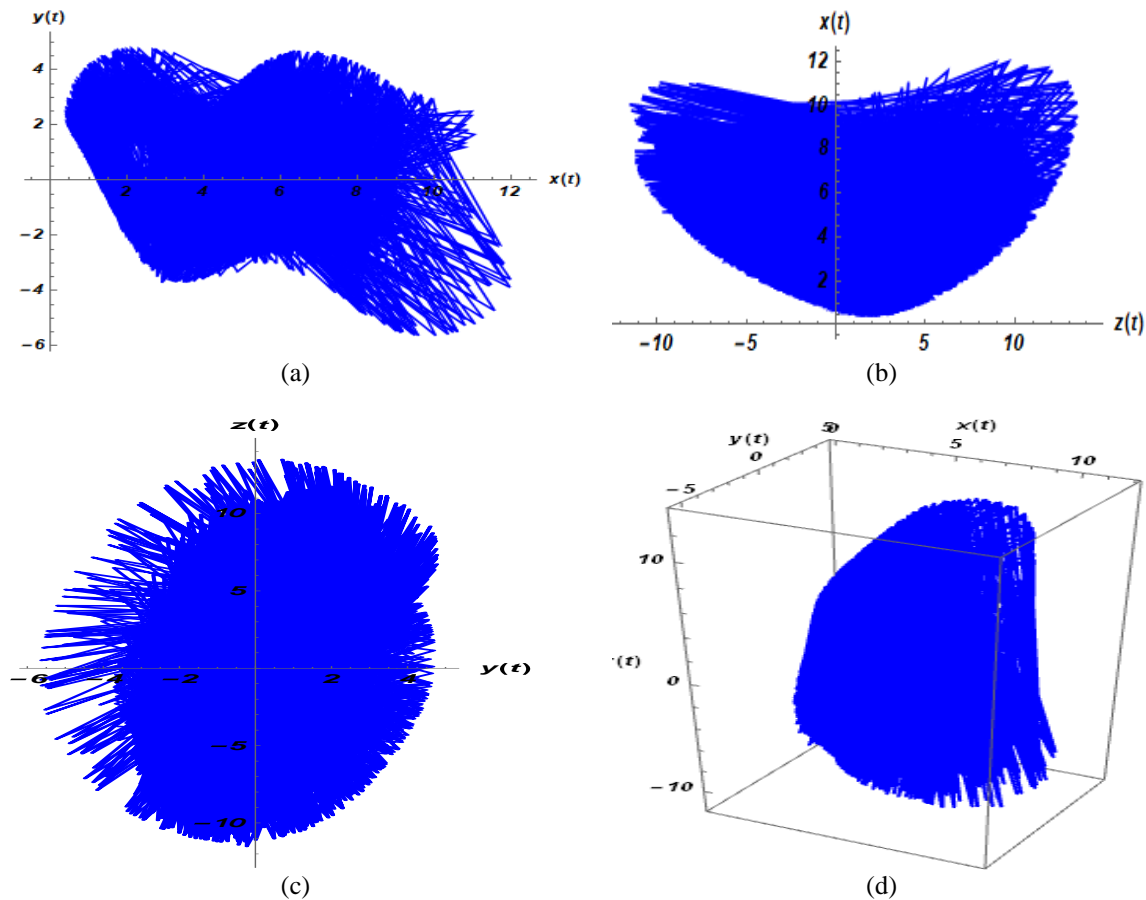


Figure 1. Attractors portrait (a) (x, y), (b) (z, x), (c) (x, z) in 2D space, and (d) (x, y, x) in 3D space

$$372.971 - 55.908\lambda - 14.5\lambda^2 - \lambda^3 = 0 \quad (2)$$

We obtain the Routh-criterion [14] from (2), $a_0 = 372.971$, $a_1 = -55.908$, $a_2 = -14.5$ and, $a_3 = -1$, $b_1 = a_1 - \frac{a_3 a_0}{a_2} = -30.1859$ hence the proposed system (1) is unstable also we conclude the Hurwitz -

criterion by formed $\Delta_1 = a_2 = -14.5 < 0$, $\Delta_2 = \begin{vmatrix} a_2 & a_0 \\ a_3 & a_1 \end{vmatrix} = 0.001118 > 0$, $\Delta_3 = \begin{vmatrix} a_2 & a_0 & 0 \\ a_3 & a_1 & 0 \\ 0 & a_2 & a_0 \end{vmatrix} = 0.000044 > 0$, hence the proposed system (1) is unstable.

2.1.2. Kaplan-Yorke dimension, Lyapunov exponent and waveform test

Its estimated divergence and convergence of neighboring paths are determined by nonlinear chaos in a dynamical system called the Lyapunov exponent also defined [3], [15]. Therefore by the three Lyapunov exponents when $(\beta, \sigma, \eta, \Omega, \rho, \omega, \mu) = (1.5, 1.38, 11, 2.5, 30, 15, 5)$ and $(x(0), y(0), z(0)) = (3.6, 1, 2.6)$, are calculated by theoretical and numerical Alan Wolf analysis with step size 0.05 used Jacobian matrix after 10000 iterations, hence $L_{\lambda_1} = 2.74 > 0$, $L_{\lambda_2} = 0.0335 > 0$, and $L_{\lambda_3} = -17.249 < 0$, since $\sum_{i=1}^2 L_{\lambda_i} > 0$ and $\sum_{i=1}^3 L_{\lambda_i} < 0$ after the order $L_{\lambda_1} > L_{\lambda_2} > L_{\lambda_3}$, we obtain the proposed system (1) is hyperchaotic, and an upper bound for fractal dimensions and Hausdorff which is called is Kaplan-Yorke dimension [16] i.e. $KY_{L_\lambda} = j + \frac{1}{|L_{\lambda_{j+1}}|} \sum_{i=1}^j L_{\lambda_i}$ hence as a result of this, $KY_{L_\lambda} = 2.1608$. Figure 2 shows the Lyapunov diagram have $L_{\lambda_{1,2}} > 0, L_{\lambda_3} < 0$.

Waveform test: the waveforms [15] for the 3D proposed system (1) are included in Figure 3 in the time domain, as a result of the oscillation's aperiodicity, their time-domain features are noncyclical. Figure 3(a) shows time vs x in the proposed system (1). Figure 3(b) shows time vs y in the proposed system (1). Figure 3(c) shows time vs x in the proposed system (1).

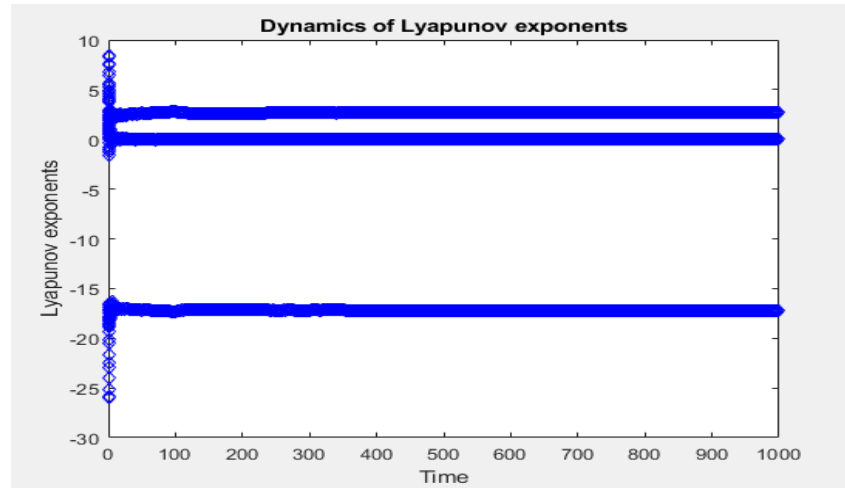


Figure 2. Lyapunov diagram by setting $(\beta, \sigma, \eta, \Omega, \rho, \omega, \mu) = (1.5, 1.38, 11, 2.5, 30, 15, 5)$

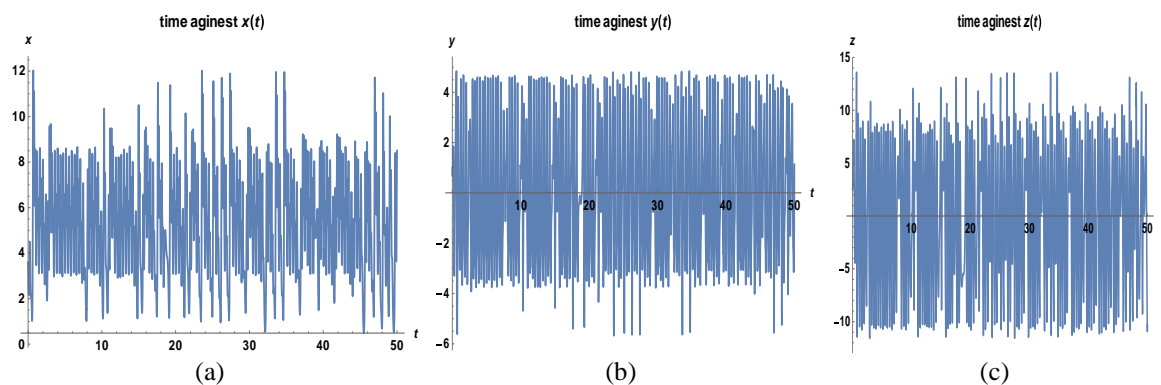


Figure 3. Waveforms for new system w.r.t (a) x , (b) y , and (c) z against time

2.2. The proposed system generated a chaotic XOR matrix_{16*16} (s-box)

Cryptography science comes to play an integral role in many applications during the ancient time in many wars. It is used mainly in the military to send a secret message from one side (sender) to another side (receiver) [17], [18]. The sender hides the original data for protecting it from unauthorized access. AES algorithm is widely used these days as a specification for the encryption by U.S NIST. It considers a much stronger than the other encryption algorithms such as DES and DES because of its block cipher, key size with 128/192/and 256 bits. The block cipher for the encrypted data is 128 bits. The basic definition of encryption is a method for protecting information such as text, documents, images, and files from changing, modification, and eavesdropping other than the intended recipient. The secret key is used by authorized people to encrypt and decrypt the data, where the sender uses one type of mathematical formula to convert the plain text to cipher text in a format that cannot be understood by the jeopardized users. The receiver performs the reverse process, taking the ciphertext and converting it to the original using the key agreed upon between the two parties. Currently, cryptography plays a major role in securely transmitting and receiving messages in online banking, telecommunications, the IoT, fog computing, and cloud computing [19]. The encryption process is classified into two types: the first one is using public and private keys, and the second is using the shared key between the two parties.

2.2.1. Proposed algorithms: the proposed XOR matrix_{16*16} consist of several points

Input the parameters $\beta, \sigma, \eta, \Omega, \rho, \omega$ and μ . and $(x(0), y(0), z(0))$ which represent the initial conditions to generate three sequences $\{(x_i, y_i \text{ and } z_i); i = 1, 2, \dots, n\}$ according to the proposed system (1). XOR between $(x_i, y_i \text{ and } z_i)$ after their conversion to unsigned 16-bit integer numbers by following the equation:

$$\begin{aligned} x_i &= \text{uint16}(x_i * 10^{10,256}) \\ y_i &= \text{uint16}(y_i * 10^{10,256}) \\ z_i &= \text{uint16}(z_i * 10^{10,256}) \end{aligned}$$

generated XOR.

The S-box new has the following properties: i) bijective, ii) the number between $(0 - 255)$ without periodic in every row and every column, and iii) 127.5 is equal to the average of all matrix_{16*16} entries. Figure 4 show the overall proposed system for the dynamic behavior with AES encryption. The only difference between a proposed XOR matrix $(16*16)$ and XOR matrix $(16*16)$ in AES [10], [20] is that the proposed XOR matrix $(16*16)$ uses integers produced from a new 3D hyperchaotic system (1). Table 1 shows the XOR matrix $(16*16)$ S-box generated based on the new 3D hyperchaotic system.

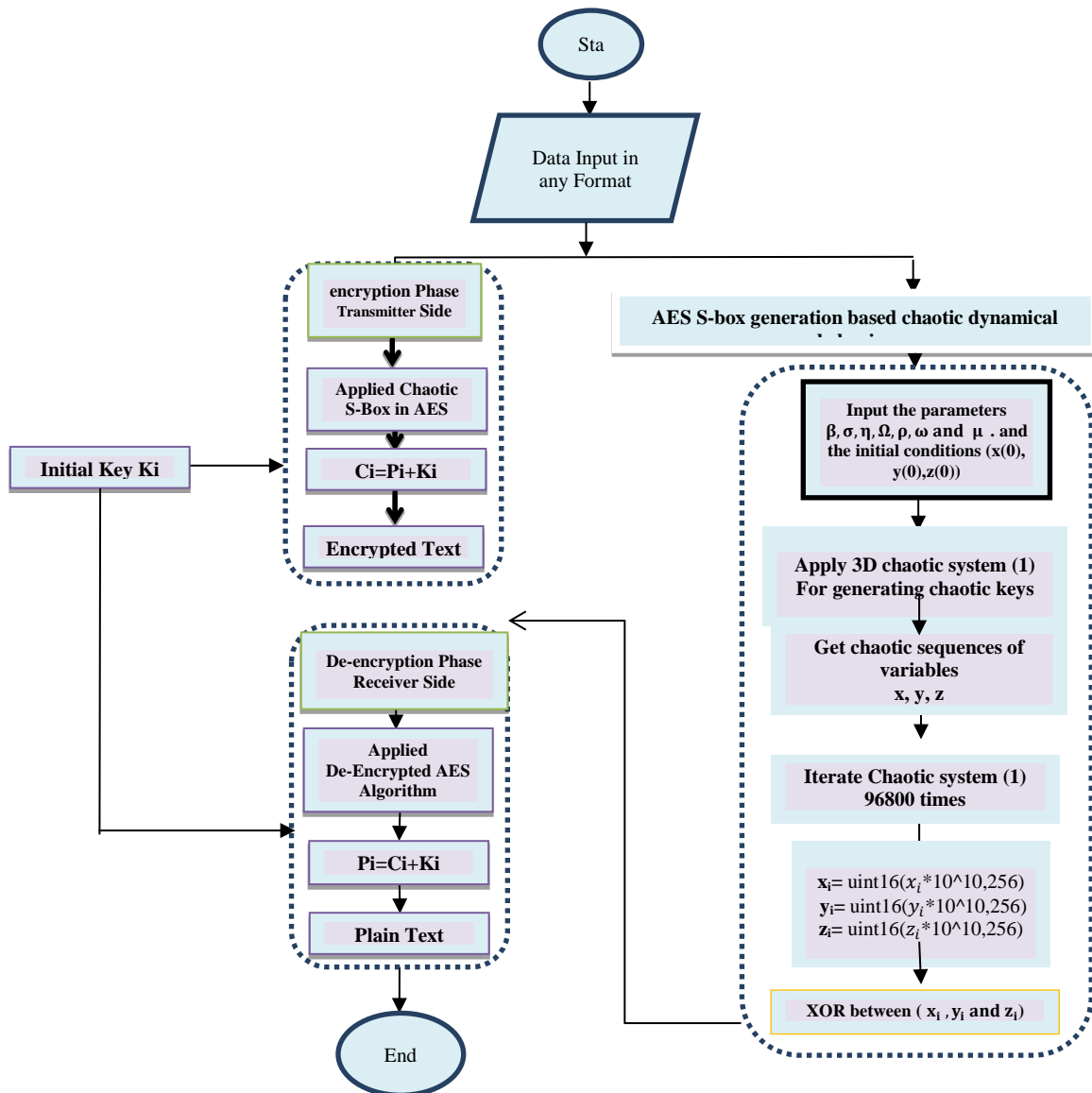


Figure 4. The overall proposed system for the dynamic behavior with AES encryption

Table 1. The proposed XOR matrix_{16*16} S-box generation

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	163	248	107	155	19	223	188	133	36	150	100	245	97	137	113	193
1	124	25	141	86	94	18	234	229	143	87	147	142	168	242	177	3
2	70	115	152	157	179	2	215	60	30	191	238	197	101	35	151	186
3	131	232	130	146	84	253	74	126	182	198	254	68	110	148	240	57
4	154	123	190	203	196	136	73	62	169	237	56	14	158	88	139	217
5	105	189	5	216	181	171	129	108	6	76	221	20	128	47	132	233
6	120	52	246	219	75	206	95	67	99	69	125	61	78	64	211	104
7	83	183	145	13	184	26	22	252	194	72	121	162	180	15	50	144
8	10	11	43	27	98	202	247	40	138	226	170	106	38	59	244	149
9	173	24	167	122	160	161	134	90	116	103	153	187	66	41	37	71
10	227	218	235	23	119	117	214	208	32	77	212	135	0	45	192	55
11	46	49	249	7	9	53	82	109	236	228	39	255	204	118	200	63
12	16	102	209	172	44	85	241	79	12	96	165	34	159	175	166	220
13	251	28	174	33	127	65	222	58	243	17	231	250	195	42	54	4
14	140	80	164	225	93	213	1	29	89	239	81	185	156	111	112	31
15	210	224	201	207	51	91	21	92	48	199	205	8	176	178	230	114

3. THE PERFORMANCE ANALYSIS OF S-BOX

The S-box generator is evaluated using many criteria. The nonlinearity provides S-box with uncertainty output, which provides counter measure to differential and linearity cryptanalysis assaults, while the strict avalanche criterion (SAC) is used for explaining the probability of each bit changing when one bit in a Boolean functions input changes is 0.5. Time is calculated to show the delay for the generation of the proposed matrix_(16*16) (S-box) based on a new 3D hyperchaotic system, In this work a new 3D hyperchaotic proposed system using $(\beta, \sigma, \eta, \Omega, \rho, \omega, \mu) = (1.5, 1.38, 11, 2.5, 30, 15, 5)$ and $(x(0), y(0), z(0)) = (3.6, 1.2, 6)$, therefore the keyspace [21] for this system by taking 15-digit precision is more than $10^{150} \approx 2^{492}$, it is very high. Also, the proposed S-box was measured and examined concerning the indicated features:

3.1. Nonlinearity

The nonlinearity is shown in [22]. We observe that the proposed matrix_{16*16} (S-box) nonlinearity rates are 110, 107, 108, 110, 108, 109, 110, and 109. We found that $min_{NL} = 107$ and $average_{NL} = 108.785$, all component functions had very large nonlinearity value. it is obvious that, the proposed (S-Box) matrix_{16*16} has excellent nonlinearity behavior.

3.2. SAC

The SAC which is shown in [22] also tested in this work for a matrix_{16*16} S-box generation based on a new 3D hyperchaotic system. Table 2 shows the main value of this test. It shows that the rate value for SAC matrix_{16*16} S – box = 0.5016, therefore any change in the input then the matrix_{16*16} (S-box) has good SAC and a decent avalanche. Table 3 shows the comparative study of the proposed matrix_{16*16} (S-box) with other references w.r.t rate value of SAC.

Table 2. SAC for the proposed XOR matrix_{16*16} S-box generation

NO.	1	2	3	4	5	6	7	8
1	0.58	0.5	0.45	0.5	0.48	0.47	0.58	0.52
2	0.44	0.48	0.48	0.47	0.5	0.5	0.48	0.53
3	0.48	0.56	0.48	0.56	0.5	0.44	0.56	0.52
4	0.5	0.52	0.48	0.5	0.48	0.52	0.47	0.52
5	0.47	0.45	0.5	0.55	0.5	0.56	0.52	0.47
6	0.44	0.48	0.47	0.53	0.47	0.47	0.52	0.52
7	0.58	0.47	0.55	0.42	0.55	0.58	0.45	0.53
8	0.48	0.53	0.53	0.45	0.48	0.44	0.56	0.53

Table 3. Comparative study of the S-box w.r.t rate value of SAC

S-box	Proposed S-box	Ref [22]	Ref [23]
rate value for SAC	0.5016	0.4976	0.4981

3.3. Time performance

One of the most components of any security is calculated to speed time. Therefore, we computed the time for the generation of the proposed matrix_{16*16} (S-box) based on a new 3D hyperchaotic system it was

discovered the technique on average a very small-time rate=0.275. The hardware used to implement this work is Intel Core i7, window 10, RAM 8 GB, 64-bit MATLAB 2019b, and mathematica 11.

4. RESULTS AND DISCUSSION

The main measurement to evaluate this work is entropy which is defined by Shanon law [24] in the (3): entropy is implemented in most cryptography systems to evaluate the randomness of the encrypted text.

$$H(x) = - \sum_{i=0}^{n-1} P(xi) \log_2(p(xi)) \quad 372.971 - 55.908\lambda - 14.5 \lambda^2 - \lambda^3 = 0 \quad (2)$$

Table 4 shows the main entropy value comparison between AES and chaotic dynamical behavior AES (CDB-AES). It is clearly shown from the table the entropy of the proposed method is close to the entropy of the AES algorithm. However, the ideal entropy value ought to be eight. If the entropy of the cipher shows a result less than eight, there exists a percentage of obviousness and the security will be a violation. The result of entropy is calculated on different message bits of the proposed and the AES algorithms using 256 different chaotic keys. Table 4 shows the comparison between the value entropy for both the proposed and the AES algorithms. The average entropy of the proposed algorithm (CBD-AES) is 7.746414. While the standard AES is 7.731757.

Table 4. Comparison between AES and improved CDB-AES

#No	AES/ entropy	CDB-AES/entropy	Message Length/bits	Chaotic K-length/bits
1.	7.2806	7.6525	128	256
2.	7.9077	7.7990	256	256
3.	7.9600	7.9866	512	256
4.	7.9009	7.9326	1024	256
5.	7.8090	7.5693	2048	256
6.	7.6796	7.6994	4096	256
7.	7.5845	7.5855	8192	256

4.1. National Institute of Standards and Technology test

The randomization of new 3D hyperchaotic keys for the proposed XOR matrix_{16*16} the process is tested by the national institute of standards and technology package for binary bits sequences [25]. Table 5 results show that the new system is passed successfully in all parameters. Therefore, the proposed XOR matrix_{16*16} has produced a sequence with excellent, arbitrary-satisfying features in all different tests.

Table 5. NIST statistical test for the improved CDB-AES

Number	NIST-800-22 Tests	P-value	Assessment
1.	Frequency (Monobit)	0.79412	Success
2.	Block Frequency (m=128)	0.10383	Success
3.	Run	0.67902	Success
4.	Discrete Fourier Transformation	0.2932	Success
5.	Non-Overlapping Template	0.42399	Success
6.	Overlapping Template	0.6876	Success
7.	Approximate Entropy	0.8941	Success
8.	Long Run	0.5113	Success
9.	Rank	0.696	Success
10.	Serial -1	0.4218	Success
	Serial -2	0.3571	Success
11.	Linear Complexity	0.6955	Success
12.	Accumulative sums (forward)	0.53789	Success
	Accumulative sums (reverse)	0.60178	Success
13.	Universal	0.83467	Success
14.	Random Excursions	0.87945	Success
15.	Random Excursions variant	0.47945	Success

5. CONCLUSION

This work introduced a 3D hyperchaotic system oscillation that is two-order autonomous and consisted of a nine-term and symmetric oscillation w.r.t x-axis used in security system with some properties that proved that the proposed system is hyperchaotic for getting more securing AES with a new XOR matrix_{16*16} (S-box) value. A novel suggestion for improving the security of the standard AES between sender




and receiver as a chaotic secure communication algorithm is implemented efficiently. This method is called CBS-AES, however, this paper generated matrix_{16*16} (S-box) have large keyspace and high nonlinear values. SAC, nonlinearity, time analysis, and NIST test were proved. The obtained matrix_{16*16} (S-box) demonstrated that all of the requirements for a decent matrix_{16*16} (S-box) were satisfied. We showed that the results can prove a way to provide high levels of security and that lead to a high level of software quality in the proposed system. In future work, S-box will be replaced with a new chaotic map.

REFERENCES




- [1] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963, doi: 10.1175/1520-0469(1963)020%3C0130:DNF%3E2.0.CO;2.
- [2] G. Chen and T. Ueta, "Yet another chaotic attractor," *Int. J. Bifurc. chaos*, vol. 9, no. 07, pp. 1465–1466, 1999, doi: 10.1142/S0218127499001024.
- [3] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Design and Analytic of A Novel SevenDimension 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.
- [4] A. Hajipour and S. S. Aminabadi, "Synchronization of chaotic Arneodo system of incommensurate fractional order with unknown parameters using adaptive method," *Optik (Stuttg.)*, vol. 127, no. 19, pp. 7704–7709, Oct. 2016, doi: 10.1016/j.ijleo.2016.06.013.
- [5] M. ElBeltagy, W. Alexan, A. Elkhayry, M. Moustafa, and H. H. Hussein, "Image Encryption Through Rössler System, PRNG S-Box and Recaman's Sequence," *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, pp. 0716–0722, doi: 10.1109/CCWC54503.2022.9720905.
- [6] H. K. Zghair, H. A. Ismael, and A. A.-H. Al-Shamery, "Image scrambler based on novel 4-D hyperchaotic system and magic square with fast Walsh–Hadamard transform," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 6, pp. 3530–3538, Dec. 2022, doi: 10.11591/eei.v11i6.4339.
- [7] O. M. Al-Hazaimah, 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.
- [8] X. Zhang, H. Zhu, and H. Yao, "Analysis of a new three-dimensional chaotic system," *Nonlinear Dyn.*, vol. 67, no. 1, pp. 335–343, 2012, doi: 10.1007/s11071-011-9981-x.
- [9] A. Lassoued and O. Boubaker, "On new chaotic and hyperchaotic systems: a literature survey," *Nonlinear Anal. Model. Control*, vol. 1, no. 6, pp. 770–789, 2016, doi: 10.15388/NA.2016.6.3.
- [10] A. I. Salih, A. Alabaichi, and A. S. Abbas, "A novel approach for enhancing security of advance encryption standard using private XOR table and 3D chaotic regarding to software quality factor," *ICIC Express Letters Part B: Applications, An International Journal of Research and Surveys*, vol. 10, no. 9, pp. 823–832, Sep. 2019, doi: 10.24507/iceilb.10.09.823.
- [11] Z. Faghani, F. Nazarimehr, S. Jafari, and J. C. Sprott, "A new category of three-dimensional chaotic flows with identical eigenvalues," *Int. J. Bifurc. Chaos*, vol. 30, no. 02, p. 2050026, 2020, doi: 10.1142/S0218127420500261.
- [12] M. Patra and S. Banerjee, "Hyperchaos in 3-D piecewise smooth maps," *Chaos, Solitons & Fractals*, vol. 133, p. 109681, Apr. 2020, doi: 10.1016/j.chaos.2020.109681.
- [13] R. M. Abdullah and A. R. Abraham, "Review of Image Encryption using Different Techniques," *Acad. J. Nawroz Univ.*, vol. 11, no. 3, pp. 170–177, 2022, doi: 10.25007/ajnu.v11n3a1301.
- [14] M. Gholami, R. K. Ghaziani, and Z. Eskandari, "Three-dimensional fractional system with the stability condition and chaos control," *Math. Model. Numer. Simul. with Appl.*, vol. 2, no. 1, pp. 41–47, 2022, doi: 10.53391/mmnsa.2022.01.004.
- [15] 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. 12051, 2021, doi: 10.1088/1742-6596/1804/1/012051.
- [16] D. Clemente-López, E. Tlelo-Cuautle, L.-G. de la Fraga, J. de J. Rangel-Magdaleno, and J. M. Munoz-Pacheco, "Poincaré maps for detecting chaos in fractional-order systems with hidden attractors for its Kaplan-Yorke dimension optimization," *AIMS Math.*, vol. 7, no. 4, pp. 5871–5894, 2022, doi: 10.3934/math.2022326.
- [17] W. Alexan, M. ElBeltagy, and A. Aboshousha, "RGB image encryption through cellular automata, s-box and the lorenz system," *Symmetry (Basel)*, vol. 14, no. 3, p. 443, 2022, doi: 10.3390/sym14030443.
- [18] T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," *Multimed. Tools Appl.*, pp. 1–25, 2022, doi: 10.1007/s11042-022-12268-6.
- [19] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e3935, 2022, doi: 10.1002/ett.3935.
- [20] H. V Gamido, M. V Gamido, and A. M. Sison, "Developing a secured image file management system using modified AES," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 4, pp. 1461–1467, Dec. 2019, doi: 10.11591/eei.v8i4.1317.
- [21] H. K. 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*, 2021, vol. 1804, no. 1, p. 12048, doi: 10.1088/1742-6596/1804/1/012048.
- [22] Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," *Symmetry (Basel)*, vol. 13, no. 4, p. 671, 2021, doi: 10.3390/sym13040671.
- [23] Y. Y. Han, Y. R. He, P. H. Liu, D. Zhang, Z. Q. Wang, and W. C. He, "Construction and application of ZUC dynamic S-box based on chaotic system. Comput," *Res. Dev.*, vol. 10, pp. 2147–2157, 2020.
- [24] A. Caplin, M. Dean, and J. Leahy, "Rationally inattentive behavior: Characterizing and generalizing Shannon entropy," *J. Polit. Econ.*, vol. 130, no. 6, pp. 1676–1715, 2022, doi: 10.3386/w23652.
- [25] M. A. I. Pekereng and A. D. Wowor, "Square transposition: an approach to the transposition process in block cipher," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 6, pp. 3385–3392, Dec. 2021, doi: 10.11591/eei.v10i6.3129.

BIOGRAPHIES OF AUTHORS






Hayder Kadhim Zghair    he received a Master's degree in Mathematics from the College of Education for Pure Sciences, Department of Mathematics, University of Babylon, Iraq in 2012. He received a Master's Ph.D., degree in Mathematics from the 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.






Mehdi Ebady Manaa    he received a Master's degree from the University Utara Malaysia (UUM), Malaysia in 2012. He received his Ph.D. in Computer Science and in the field of Network Security and Data Mining using Cloud Computing from the University of Babylon, College of Information Technology in 2016. He is currently focusing on the detection of the attacks. The main interesting fields are data mining techniques (clustering and classification), communication software, network security, cloud computing, the internet of things, and unstructured data. He can be contacted at email: it.mehdi.ebady@itnet.uobabylon.edu.iq.



Safa Saad A. Al-Murieb    she received a Master's degree in Computer Science from the Faculty of Science, University of Babylon, Iraq in 2011. She received her Ph.D. degree in Computer Science from the Faculty of the Information Technology University of Babylon, Iraq in 2017. Her research interests include multimedia, data security, and AI. She can be contacted at email: safa.abbas@uobabylon.edu.iq.



Fryal Jassim Abd Al-Razaq    she received a Bachelor's degree in computer science from the College of Science, Department of Computer Science, University of Basrah, Iraq in 2002. She received a Master's degree in Computer Science from the Faculty of Science, University of Babylon, Iraq in 2014. Her research interests include data mining techniques (clustering and classification). She can be contacted at email: fryal.jassim@uobabylon.edu.iq.