TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 20, No. 6, December 2022, pp. 1230~1238
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v20i6.23449

A dynamic S-box generation based on a hybrid method of new chaotic system and DNA computing

Huda Rashid Shakir, Sadiq Abdul Aziz Mehdi, Anwar Abbas Hattab
Department of Computer Science, Collage of Education, Mustansiriyah University -Iraq, Baghdad, Iraq

Article Info

Article history:

Received Feb 25, 2022
Revised Sep 06, 2022
Accepted Sep 16, 2022

Keywords:

Balanced
Bit independence criteria
DNA computing
Hyper-chaotic system
Strict avalanche criteria
Substitution box

ABSTRACT

S-box is one of the most significant structures used to construct encryption that is strong and resistant to attacks in encryption algorithms. The new 4D-hyper chaotic system and deoxyribonucleic acid (DNA) computing are used in this paper to provide a new dynamic S-box generating approach. The 4D generated numbers are processed to generate a hexadecimal number that will encode using the DNA coding method and using addition, subtraction, and exclusive-or operations to produce the final DNA string decoded to make the S-Box. The dynamic form of s-boxes is represented by a minor change in the initial conditions of the proposed chaotic method that will generate dynamic sequences of numbers. The proposed method enhances the security criteria of the block ciphers. The S-box testing criteria were done like strict avalanche, balanced, and bit independence criteria, in addition to differential approximation probability and linearity approximation probability, to test the security of the new S-Box. The results show that the new S-box has good security and is resistant to attacks.

Corresponding Author:

Huda Rashid Shakir
Department of Computer Science, Collage of Education, Mustansiriyah University -Iraq
Alkadhimiya Street, Baghdad, Iraq
Email: hudarashid@uomustansiriyah.edu.iq

1. INTRODUCTION

Data security is becoming increasingly important. To keep data safe, new encryption methods and algorithms have been developed. Studies of encryption using chaotic systems are an alternative to modern encryption algorithms [1]. The properties of chaos systems' unique features, such as unpredictability, initial conditions, ergodicity, high sensitivity, deterministic behavior, and pseudo randomness, perfectly match cryptography's fundamental requirements [2], [3]. A chaotic system is a nonlinear system that has just one positive Lyapunov exponent, whereas a hyperchaotic system has more than positive Lyapunov exponent. Thus, in contrast to the chaotic attractor, the hyperchaotic attractor is deployed in multiple directions, whereas the chaotic attractor is deployed in a single direction [4]. Recently, the use of chaos in the cryptography and telecommunications area has become popular [5], [6].

On the other hand, DNA cryptography is an area of biological science that can store a significant amount of data, has strong parallel processing, and very low power consumption [7], [8]. It stores information about living organisms. The genetic material in living organisms is called deoxyribonucleic acid (DNA), and it is responsible for passing genetic traits from one generation to the next. DNA is a polymer made up of nucleotides. Each nucleotide has three parts: a nitrogenous base, a phosphate group, and a deoxyribose sugar. The nitrogenous bases are adenine, thymine, guanine, and cytosine. Watson and Crick's complementary DNA structure is used for DNA computing. Algebraic operations, such as DNA bases, DNA addition, DNA subtraction, and a DNA execlusive-or (XOR) function, are used to express biological characteristics [9]-[11].

Creating S-boxes with powerful cryptographic features is an important stage in designing block cipher systems. Substitution-boxes are non-linear components of block cryptosystems that play an essential role in the security of cryptosystems. The origins of the S-box can be traced back to Shannon's cryptographic substitution. Two types of S-box exist: static S-boxes, in which the input vector remains constant, and dynamic S-boxes, in which input values fluctuate, resulting in changes to the corresponding output. As a result, the idea is to create dynamic S-boxes using the chaotic system and DNA computing [5], [12].

In the last years, there have been some S-box design algorithms developed based on chaotic systems and DNA computation. Masood *et al*. [13], presented an approach that integrates DNA sequencing code, Arnold transformation, and a chaotic dynamical system to produce an initial S-box. A number of experiments have been performed in order to verify the randomness of this newly generated S-box. These tests involve the strict avalanche criterion, nonlinearity analysis, and bit independence criterion. The results indicate that the proposed method has a strong ability to resist many attacks. Al-Wattar *et al.* [14], suggested building a new substitution box for substitution–permutation network (SPN) symmetric block ciphers inspired by DNA biology techniques.

Lu *et al*. [15], a new algorithm for constructing S-boxesare proposed that is based on a new compound chaotic system. The original S-box was Zcreated using the novel linear mapping, and the initial S-box was scrambled using the the tent logistic system (TLS). The efficiency of creating S-boxeswas improved, as were the cryptographic properties of the S-Box. The suggested S-box had a higher linear probability (LP) and differential probability (DP) score than other previous S-Boxes, indicating that the suggested S-box had evident advantages in repelling differential and linear cryptanalysis attacks. Lambić [16], offered a new way for creating random bijective S-boxes based on an enhanced one-dimensional discrete chaotic map.

Yang *et al.* [17], created a new S-box by selectively self-scrambling a number of initial S-boxes formed by the chaotic sequence of a two-dimensional multiple collapse chaotic map (2D-MCCM). Several S-box tests have been conducted, such as nonlinearity, completeness, strict avalanche criterion, and differential approximation probability, such as balanced, avalanche criterion, completeness, and strict avalanche criterion. The performance analysis of the S-box showed that it can withstand a wide range of security attacks.

The motivation for this paper is to build a robust dynamic S-box with good encryption by exploiting the good features of chaotic systems, such as randomlike behavior, ergodic behavior, and sensitivity to initial conditions, as well as the advantages of DNA computing, like strong parallel processing, very low power consumption, and large data storage capacity. So, four chaotic sequences are used to increase the difficulty of predicting dynamic behaviors and randomness. Additionally, the chaotic attractor becomes more complex.

The main contribution is the construction of dynamic S-boxesmethod with a cryptographically keyed strong, based on a new 4D chaotic system and DNA computing, which can satisfy six criteria of S-Box. In this paper, we present a new dynamic S-box generation algorithm design based on the new 4D-hyper chaotic system and DNA computing. Different security criteria were evaluated. These included the bijective, strict avalanche, balanced and bit independence creteria.

2. THEORETICAL BACKGROUND

2.1. DNA coding

In 1994, the first DNA computing experiment was done by Adleman. Several researchers have found that DNA computing has a lot of characteristics such as massive storage capacity, low power consumption, and parallel computing ability. DNA molecules consist of the four different DNA nucleotides called adenine (A), cytosine (C), guanine (G), and thymine (T). In a complementary pairing, the nucleotides A and T, as well as G and C, form a pair. The decimal digits 0 to 3 can be represented by the letters A, T, G, and C. The binary digits 00, 01, 10, and 11 can be used to represent these four decimal digits, allowing each nucleotide to carry two bits of data. In total, there are 4! = 24 different ways to encode data using this coding scheme. In contrast, there are only eight types of encoding methods that follow the rule of complementing pairs [18]-[20]. The eight types of encoding are given in Table 1, and the operations DNA (addition, subtraction, and x-or) are shown in Table 2.

2.2. The novel chaotic system

A new 4D-hyper chaotic system is constructed using a system model represented by the following differential equation.

$$
\begin{aligned}
\frac{dx}{dt} &= -a\,x - b\,w + c\,y\,z + z\,e^{y} \\
\frac{dy}{dt} &= d\,y + e\,x - f\,x\,z - x\,e^{z} \\
\frac{dz}{dt} &= -\,g\,z + h\,x\,y \\
\frac{dw}{dt} &= -b\,w + i\,x\,z + j\,y\,z
\end{aligned}
\tag{1}
$$

Where x, y, z, w is called the states of system, $t \in \Re$ and $a, b, c, d, e, f, g, h, i$ and j are positive parameters of the system (1) shows a chaotic attractor in a new four-dimensional chaotic system with parameter values of: $a = 3.1$, $b = 2.1$, $c = 15.8$, $d = 1.1$, $e = 16.5$, $f = 1.5$, $g = 2.4$, $h = 26.6$, $i = 5.1$ and $j = 12.9$, and the initial conditions as: $x(0) = 0.2, y(0) = 0.4, z(0) = 1.5$ and $w(0) = 0.8$.

Table 1. DNA rules [21]

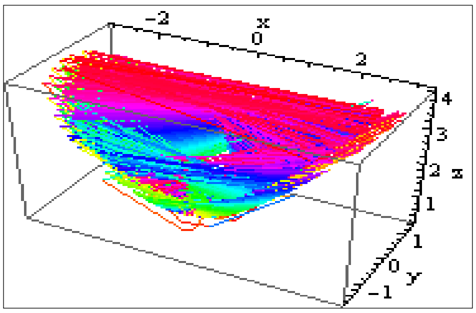
Rules	1	2	3	4	5	6	7	8
0	A	A	C	C	G	G	T	T
1	G	C	T	A	T	A	G	C
2	C	G	A	T	A	T	C	G
3	T	T	G	G	C	C	A	A

Table 2. The operation of DNA sequences [21]

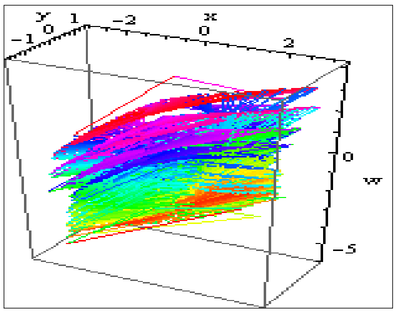
Addition-DNA					Subtraction-DNA					Exclusive-or				
(Add)	A	C	G	T	(Sub)	A	C	G	T	(Xor)	A	C	G	T
A	T	A	C	G	A	C	A	T	G	A	A	C	G	T
C	A	C	G	T	C	G	C	A	T	C	C	A	T	G
G	C	G	T	A	G	T	G	C	A	G	G	T	A	C
T	G	T	A	C	T	A	T	G	C	T	T	G	A	C

2.3. Lyapunov exponent

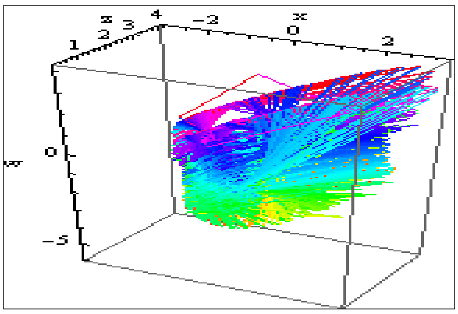
Calculating the Lyapunov exponent, according to nonlinear dynamical theory, is a quantitative measure of the sensitive dependency on the initial values. It's the average rate at which two adjacent trajectories diverge (or converge). When the system's parameters (1) are chose as: (a = 3.1, b = 2.1, c = 15.8, d = 1.1, e = 16.5, f = 1.5, g = 2.4, h = 26.6, i = 5.1, and j = 12.9), as well as the initial values as: $LE1$ = 4.05761, $LE2$ = 0.347562, $LE3$ = -3.94257 and $LE4$ = -6.61896. This system contains chaotic features since the highest Lyapunov exponent is positive. Because $LE1$ and $LE2$ are positive Lyapunov exponents, and the two remainders are negative. As a result, the system is hyper-chaotic. Figure 1(a) show the system's attractors in $(x - y - z)$, Figure 1(b) in $(y - x - w)$, and Figure 1(c) $(x - z - w)$.



(a)



(b)



(c)

Figure 1. Chaotic attractors, three dimensional view: (a) $(x - y - z)$, (b) $(y - x - w)$, and (c) $(x - z - w)$

3. METHODOLOGY

The proposed method is represented by applying a hybrid method to generate dynamic substitution boxes that are stronger for increasing secrecy. The method used a new chaotic system (four-dimension) for key generation, then converting it to DNA coding and using DNA operations (addition, subtraction, and xor) to produce new S-box more security. The total steps are shown in Figure 2.

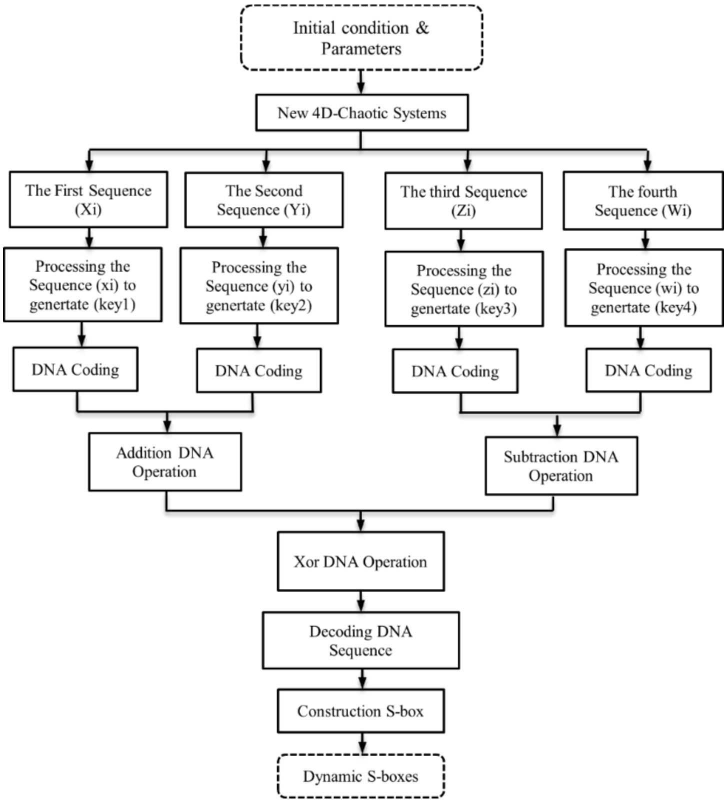


Figure 2. The framework of the proposed method

3.1. Chaotic sequence generation stage (key generation)

In this step, four chaotic sequences are generated based on the initial conditions and parameters that belong to the novel 4-D hyper-chaotic system (1). The proposed hyper-chaotic system iterates to create four chaotic sequences (xi, yi, zi, wi) of real numbers, which are converted into four vectors ($key1$, $key2$, $key3$, $key4$) from the chaotic sequence. The Algorithm 1 describes the steps of chaotic key generation, and the Table 3 shows the processing of the values that are generated from chaotic sequences.

Algorithm 1. Key generation

Input: $x(0)$, $y(0)$, $z(0)$ and $w(0)$ and system parameters a, b, c, d, e, f, g, h, i and j
Output: $key1$, $key2$, $key3$, $key4$
Begin
Step 1: Specifying empty string $key1$, $key2$, $key3$, and $key4$
Step 2: For $i \leftarrow 1$ to n
    Using (1) for find xi, yi, zi, and wi
    Getting the absolute value of each number for xi, yi, zi, and wi
    Getting the remaining one of each number for xi, yi, zi, and wi
    Removing the floating-point and getting the fixed number of digits for xi, yi, zi, and wi
    Converting to hexadecimal for xi, yi, zi, and wi
    Concatenation with the string $key1$, $key2$, $key3$, $key4$
    Next i
Step 3: Return $key1$, $key2$, $key3$, $key4$
End algorithm

Table 3. The processing of chaotic generating numbers

Generated no.	The remaining of 1	Remove floating point	Hexadecimal form
0.295698	0.29570	295698398405	‘44D8FF7CC5’
0.396147	0.39615	396146903920	‘5C3C320B70’
0.504490	0.50449	504489871284	‘7575F087B4’
0.624383	0.62438	624383033645	‘916021012D’
0.759960	0.75996	759960212958	‘B0F12895DE’
0.916840	0.91684	916840383140	‘D577F202A4’
1.102246	0.10225	102246038250	‘17CE56BAEA’
1.324952	0.32495	324952491840	‘4BA8AD8740’

3.2. S-boxes generation

At this stage, we proposed new S-boxes based on a hybrid method combining a chaotic system with DNA encoding. Initially, based on the chaotic sequences ($key1$, $key2$, $key3$, $key4$) that were generated from the previous stage, additionally, algebraic DNA operations (addition, subtraction, and exclusive-or) are used to make a set of S-boxes with a size of (16×16). Each chaotic sequence is converted into a binary string, which is then transformed into DNA sequences based on Table 1, so that each 2 bits is substituted with one DNA code, such as 00 is replaced by A, 01 by C, 10 by G, and 11 by T. Table 4 shows a sample of transformed chaotic sequences into DNA coding.

The addition operation is performed between the first and second sequences ($key1$, $key2$) based on addition-DNA in Table 2, while the subtraction operation is performed between the third and fourth sequences ($key3$, $key4$) based on subtraction-DNA in Table 2. Finally, the XOR operation is applied between the results of the previous addition and subtraction steps based on Table 2. The output of these operations is used to generate a set of S-boxes, with each digit represented as one cell in the S-box. This value should not be repeated in the S-box. It is checked whether or not the created value exists in the S-box. If this is a generated value that was previously present in the S-box, it is discarded. If it does not exist in the S-box, a new value is added, and this process is repeated until the S-box values are unique 256 values. The S-box values results are shown in Table 5.

Table 4. The DNA coding sample

Generate sequence	DNA coding
2E90EDD00044D8FF7CC55C3C32	AGTGGCAATGTCTCAAAAAACACA TCGATTTTCTTATACCCCTAATTAAT

Table 5. The hexadecimal of S-box values results

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	32	29	21	24	5B	B1	33	15	76	19	9F	ED	3E	01	A9	67
1	57	C8	27	04	28	F6	E5	D5	8B	6E	86	45	BE	77	EB	8E
2	11	46	AA	61	C2	93	03	D3	87	02	8F	F3	74	05	23	43
3	4E	A7	79	91	CC	25	2A	84	8C	BC	8D	5A	39	0E	C9	12
4	59	85	14	C4	CD	B9	BF	75	D2	E4	83	38	C5	B3	F9	20
5	34	B5	FA	42	2F	00	52	A6	53	C7	3A	AF	64	D8	B6	71
6	B0	2D	CA	37	30	9D	B2	B8	0C	58	EF	E8	F8	2C	06	63
7	66	7A	EE	A3	16	80	A8	5C	2B	BB	62	0B	48	4A	18	99
8	A5	CF	D7	22	94	1A	96	95	E3	7F	C0	40	6B	D1	5F	78
9	AB	60	E7	F1	C6	D4	A4	FE	2E	EC	FD	51	E6	7D	8A	F5
A	A1	07	C3	1F	26	4B	E9	4D	1E	47	41	BD	9E	A2	6A	13
B	92	CB	3D	3C	F4	56	D0	7B	DE	E0	B4	97	CE	9C	4F	98
C	C1	FC	5E	36	55	F2	08	F0	FF	44	7C	D6	F7	0F	6F	6D
D	7E	9A	35	DA	31	D9	9B	3B	E1	69	E2	AD	DD	10	68	82
E	EA	DB	73	88	4C	0D	1C	AE	09	6C	0A	1D	AC	17	BA	89
F	3F	72	DC	90	50	1B	49	65	5D	81	A0	FB	70	54	DF	B7

4. RESULTS AND DISCUSSION

The design of cryptographically good S-boxesis built on essential criteria. For instance, balanced, strict avalanche, bit independence creteria, differential probability, as well as linear probability. The evaluation criteria are discussed in the following subsections.

Table 6. Balanced criteria test

No. S-box	BC (computer)	
	No. 0’s	No. 1’s
1	32	32
Ref [23]	33	31

4.1. Balanced criteria

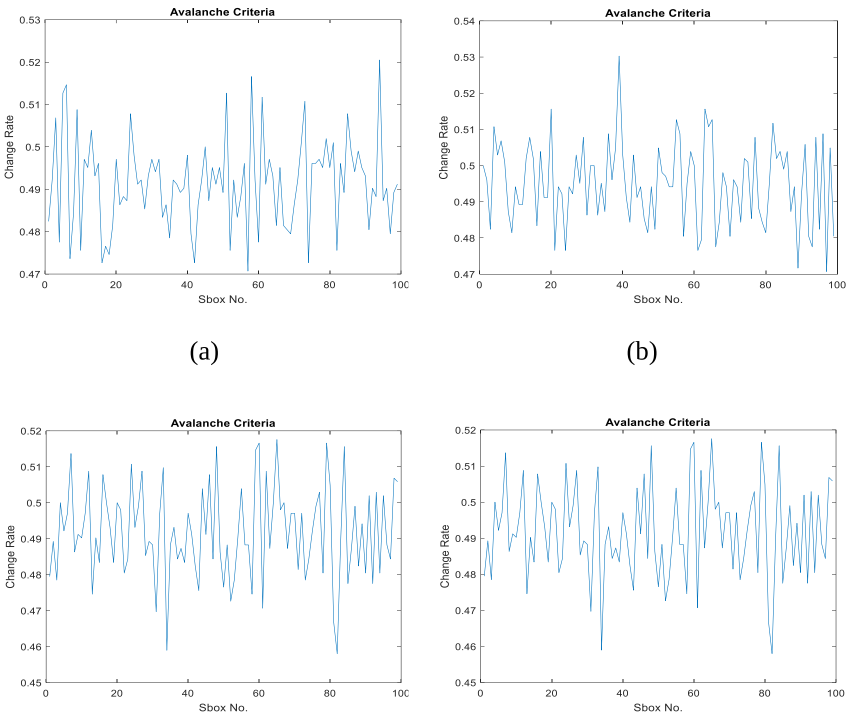
A balanced distribution of 0 and 1 values output sequence is a crucial requirement for the S-box [14], [22]. According to this evaluation, the S-boxes formed by our suggested method are balanced since they include equal values of 0's and 1's. This test is represented by comparing the number of zeros and the number of ones in the generated sequence. In the proposed method, the total ones are equal to the number of zeros in all generated S-boxes as shown in Table 6, which illustrates the balanced test for the word "computer" using 6-S-box generating.

4.2. The bijective property

An $(n \times n)$ S-box is bijective if it contains all possible output values between $[0, 2n - 1]$ [24], [25]. Because the produced S-box contains all different values in the interval $[0;\ 255]$, it satisfies the requirements of the bijectivity property. The value of all constructed S-boxes is 128. This is the same as the ideal value. All of the S-boxes were analyzed and verified that all of them were bijective.

4.3. Strict avalanche criteria (SAC)

In Çavuşoğlu *et al.* [1] and Faheem *et al.* [26] SAC is a performance criterion introduced by Webster and Tavares. That is, when an input bit changes, half of each output bit changes too. The estimated value of 0.5 is optimal. The S-box meets the SAC requirement if the estimated value is close to 0.5 as shown in Table 7, and the avalanche criteria of the proposed method are seen in Figure 3(a) which shows the first dimension, Figure 3(b) second dimension, Figure 3(c) third dimension, and Figure 3(d) fourth dimension.



(a) (b)

(c) (d)

Figure 3. The avalanche criteria of the proposed method (a) first dimension, (b) second dimension, (c) third dimension, and (d) fourth dimension

Table 7. SAC of the proposed S-box

SAC							
0.4824	0.4824	0.4824	0.4824	0.4824	0.4824	0.4824	0.4824
0.4921	0.4921	0.4921	0.4921	0.4921	0.4921	0.4921	0.4921
0.5068	0.5068	0.5068	0.5068	0.5068	0.5068	0.5068	0.5068
0.4775	0.4775	0.4775	0.4775	0.4775	0.4775	0.4775	0.4775
0.5126	0.5126	0.5126	0.5126	0.5126	0.5126	0.5126	0.5126
0.5146	0.5146	0.5146	0.5146	0.5146	0.5146	0.5146	0.5146
0.4736	0.4736	0.4736	0.4736	0.4736	0.4736	0.4736	0.4736
0.4843	0.4843	0.4843	0.4843	0.4843	0.4843	0.4843	0.4843

4.4. Bit independence criteria

In Çavuşoğlu *et al.* [1] the approach of independent output bits, introduced by Webster and Tavares, is another way to evaluate the performance of S-boxes. Using this method determines whether a set of vectors formed with the reverse bit of plain text is independent of all avalanche variable sets. Table 8 shows the bit independence criterion of the suggested S-box.

Table 8. Bit independence criterion of the suggested S-box

BIC							
0.4971	0.4971	0.4971	0.4971	0.4971	0.4971	0.4971	0.4971
0.4927	0.4927	0.4927	0.4927	0.4927	0.4927	0.4927	0.4927
0.4956	0.4956	0.4956	0.4956	0.4956	0.4956	0.4956	0.4956
0.4937	0.4937	0.4937	0.4937	0.4937	0.4937	0.4937	0.4937
0.5039	0.5039	0.5039	0.5039	0.5039	0.5039	0.5039	0.5039
0.4888	0.4888	0.4888	0.4888	0.4888	0.4888	0.4888	0.4888
0.4956	0.4956	0.4956	0.4956	0.4956	0.4956	0.4956	0.4956
0.5068	0.5068	0.5068	0.5068	0.5068	0.5068	0.5068	0.5068

4.5. Correlation

A correlation value must be measured to determine the correlation between avalanche variable sets, as shown in Table 9. Table 9 indicates the correlation between samples (8 S-boxes) except for the sample with itself, which indicates the diagram is zero. All the results explain that there is no correlation between the S-box and other ones.

Table 9. The correlation between avalanche variable sets

No. S-box	1	2	3	4	5	6	7	8
1	0.0000	0.0374	0.1261	0.0026	0.0034	0.0492	0.1103	-0.0381
2	0.0374	0.0000	-0.0418	-0.0258	-0.0160	0.0872	-0.0734	-0.0306
3	0.1261	-0.0418	0.0000	-0.0494	-0.0515	-0.0172	0.0655	0.0848
4	0.0026	-0.0258	-0.0494	0.0000	0.0433	-0.0100	0.0864	0.0846
5	0.0034	-0.0160	-0.0515	0.0433	0.0000	-0.0254	0.0173	0.1327
6	0.0492	0.0872	-0.0172	-0.0100	-0.0254	0.0000	-0.0409	-0.0688
7	0.1103	-0.0734	0.0655	0.0864	0.0173	-0.0409	0.0000	0.0453
8	-0.0381	-0.0734	0.0848	0.0846	0.1327	-0.0688	0.0453	0.0000

4.6. Differential approximation probabilities

A differential cryptanalysis approach was introduced by Biham and Shamir. The DP approach calculates the XOR distribution between the input and output bits of the S-box. The S-box will be resistant to differential attack if the distribution between the input and output bits is close. The definition of DP.

$$DP = max_{\Delta_x \neq 0, \Delta y}(\# x \in X, f_x \oplus f(x + \Delta_x) = \Delta_y / 2^n \quad (2)$$

Where X denotes the set of all possible input values and $2n$ the number of its elements, a strong S-box should have a DP value close to zero [27]. Table 10 presents the differential probability matrix of the suggested S-box, and the highest value is 10. Furthermore, from the (2), the maximum DP value of the proposed S-box can be calculated to be 0.03921, which is close to zero, which shows that it is very resistant to different attacks.

Table 10. The proposed S-Box’s differential approximation probability

DP							
8	6	6	6	6	6	8	6
8	6	6	6	8	6	8	8
6	6	6	8	6	8	8	8
6	10	8	6	8	6	6	6
6	6	6	6	8	6	8	8
8	6	6	6	6	8	6	6
6	8	10	8	8	8	6	6
8	6	6	6	6	10	10	6

4.7. Linear approximation probability

The probability of a linear approximation LP is defined.

$$LP_f = max_{a,b \neq 0}(\frac{\#\{x \in X | x.a = f(x).b\} - 2^{n-1}}{2^n} \quad (3)$$

Where a, b are the input and output masks, respectively [28]. According to Table 11, the proposed S-box has a smaller LP value, which indicates it is more resistant to linear cryptanalysis. Table 11 displays the linear approximation probability of construction S-boxes.

Table 11. Linear approximation probability of construction S-boxes

a	b	LP
117	128	0.011719
122	98	0.003906
111	99	0.011719
131	34	0.007813
88	83	0.007813
158	138	0.003906
88	83	0.007813
108	248	0.003906

4.8. Comparison

Table 12 shows the comparative between our proposed method with the related works: [13], [15]-[17]. The results show that our S-box has smaller values of LP and DP than the other S-boxesin comparable related work. Furthermore, the mean SAC value (0.5205) of our suggested S-boxesis very close to the optimal value of 0.5. In addition, the mean value of the bit independence criterion (BIC) is 0.5317, which is also near the ideal value of 0.5.

Table 12. Comparison proposed method with other methods

S-box	BIC	SAC	Max differential probability	Linearity probability
Ref. [13]	-	0.5547	0.039	0.1560
Ref. [15]	0.499	0.505	0.039	0.125
Ref. [16]	-	0.0295	-	-
Ref. [17]	0.5008	0.5313	0.0391	0.1250
Proposed	0.5317	0.5205	0.03921	0.011719

5. CONCLUSION

Substitution boxes are critical nonlinear elements for modern block and stream ciphers to achieve cryptanalytic resistance. In this paper, the new 4D hyper-chaotic system is utilized to produce S-boxes. The hyper-chaotic system with more sophisticated behaviors offers sufficient randomness to generate stronger keys. In addition, it utilizes DNA encoding to achieve better security. Several tests have been performed to measure the performance of the proposed S-box. The test results and performance analysis illustration that our proposed S-box is balanced and has very smaller values of LP and DP. This means the proposed S-boxesare very secure against linear and differential attacks.

REFERENCES

[1] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear dynamics*, vol. 87, pp. 1081–1094, 2017, doi: 10.1007/s11071-016-3099-0.

[2] S. A. Mehdi and A. A. Kadhim, "Image Encryption Algorithm Based on a New Five Dimensional Hyperchaotic System and Sudoku Matrix," *2019 International Engineering Conference (IEC)*, 2019, pp. 188-193, doi: 10.1109/IEC47844.2019.8950560.

[3] 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, 2019, doi: 10.1515/jisys-2018-0404.

[4] A. N. Mouelas, T. F. Fozin, R. Kengne, J. Kengne, H. B. Fotsin, and B. Z. Essimbi, "Extremely rich dynamical behaviors in a simple nonautonomous Jerk system with generalized nonlinearity : hyperchaos, intermittency, offset-boosting and multistability," *International Journal of Dynamics and Control*, vol. 8, no. 1, pp. 51–69, 2020, doi: 10.1007/s40435-019-00530-z.

[5] B. Idrees, S. Zafar, T. Rashid, and W. Gao, "Image encryption algorithm using S-box and dynamic Hénon bit-level permutation," *Multimedia Tools and Applications*, vol. 79, pp. 6135–6162, 2020, doi: 10.1007/s11042-019-08282-w.

[6] S. Vaidyanathan, A. Sambas, S. Zhang, Y. Zeng, M. A. Mohamed, and M. Mamat, "A new two-scroll chaotic system with two nonlinearities: Dynamical analysis and circuit simulation," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2465–2474, 2019, doi: 10.12928/TELKOMNIKA.v17i5.10650.

[7] V. R. F. Signing, R. L. T. Mogue, J. Kengne, M. Kountchou, and Saïdou, "Dynamic phenomena of a financial hyperchaotic system and DNA sequences for image encryption," *Multimedia Tools and Applications*, vol. 80, pp. 32689–32723, 2021, doi: 10.1007/s11042-021-11180-9.

[8] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, "A comparative review on symmetric and asymmetric dna-based cryptography," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 6, pp. 2484–2491, 2020, doi: 10.11591/eei.v9i6.2470.

[9] G. Zhong, T. Li, W. Jiao, L. N. Wang, J. Dong, and C. L. Liu, "DNA computing inspired deep networks design," *Neurocomputing*, vol. 382, pp. 140–147, 2020, doi: 10.1016/j.neucom.2019.11.098.

[10] Q. Ma, C. Zhang, M. Zhang, D. Han, and W. Tan, "DNA Computing: Principle, Construction, and Applications in Intelligent Diagnostics," *Small Structures*, vol. 2, no. 11, 2021, doi: 10.1002/sstr.202100051.

[11] D. D. Khudhur and M. S. Croock, "Physical cyber-security algorithm for wireless sensor networks," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 4, pp. 1177-1184, 2021, doi: 10.12928/TELKOMNIKA.v19i4.18464.

[12] A. Jain, P. Agarwal, R. Jain, and V. Singh, "Chaotic Image Encryption Technique using S-box based on DNA Approach,"

International Journal of Computer Applications, vol. 92, no. 13, pp. 30–34, 2014, doi: 10.5120/16070-5225.
[13] F. Masood *et al*., "A new color image encryption technique using DNA computing and Chaos-based substitution box," *Soft Computing*, vol. 26, pp. 7461–7477, 2022, doi: 10.1007/s00500-021-06459-w.
[14] A. H. S. Al-Wattar, R. Mahmod, Z. Zukarnain, and N. I. Udzir, "Generating a new S-Box inspired by biological DNA," *International Journal of Computer Science and Application*, vol. 4, no. 1, pp. 32–42, 2015. [Online]. Available: https://www.researchgate.net/publication/281507513_Generating_a_new_S-Box_inspired_by_biological_DNA
[15] Q. Lu, C. Zhu, and G. Wang, "A Novel S-Box Design Algorithm Based on a New Compound Chaotic System," *Entropy*, pp. 1–15, 2019, doi: 10.3390/e21101004.
[16] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *Journal of Information and Telecommunication*, vol. 2, no. 2, 2018, doi: 10.1080/24751839.2018.1434723.
[17] C. Yang, X. Wei, and C. Wang, "S-box design based on 2d multiple collapse chaotic map and their application in image encryption," *Entropy*, vol. 23, no. 10, 2021, doi: 10.3390/e23101312.
[18] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," *in IEEE Access*, vol. 8, pp. 88093-88107, 2020, doi: 10.1109/ACCESS.2020.2990170.
[19] G. Cui, L. Wang, X. Zhang, and Z. Zhou, "An Image Encryption Algorithm Based on Dynamic DNA Coding and Hyper-chaotic Lorenz System," *International Conference on Bio-Inspired Computing: Theories and Applications*, Singapore: Springer, 2018, doi: 10.1007/978-981-13-2829-9.
[20] B. K. Siddartha and G. K. Ravikumar, "An efficient data masking for securing medical data using DNA encoding and chaotic system," *International Journal of Electrical & Computer Engineering*, vol. 10, no. 6, pp. 6008-6018, 2020, doi: 10.11591/ijece.v10i6.pp6008-6018.
[21] A. Girdhar and V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimedia Tools and Applications*, vol. 77, pp. 27017–27039, 2018, doi: 10.1007/s11042-018-5902-z.
[22] Z. Jiang, and Q. Ding. "Construction of an S-box based on chaotic and bent functions," *Symmetry*, vol. 13, no. 4, 2021, doi: 10.3390/sym13040671.
[23] B. Maram K. and J. M. Gnanasekar, "Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output," *TEM Journal*, vol. 5, no. 1, pp. 67–75, 2016, doi: 10.18421/TEM51-11.
[24] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons and Fractals*, vol. 58, pp. 16–21, 2014, doi: 10.1016/j.chaos.2013.11.001.
[25] X. Liu, X. Tong, Z. Wang, and M. Zhang, "Efficient high nonlinearity S-box generating algorithm based on third-order nonlinear digital filter," *Chaos, Solitons & Fractals*, vol. 150, 2021, doi: 10.1016/j.chaos.2021.111109.
[26] Z. B. Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, "Highly dispersive substitution box (S-box) design using chaos," *ETRI Journal*, vol. 42, no. 4, pp. 619–632, 2020, doi: 10.4218/etrij.2019-0138.
[27] N. Hematpour and S. Ahadpour, "Execution examination of chaotic S-box dependent on improved PSO algorithm," *Neural Computing and Applications*, vol. 33, no. 10, pp. 5111–5133, 2021, doi: 10.1007/s00521-020-05304-9.
[28] H. Zhu, X. Tong, Z. Wang, and J. Ma, "A novel method of dynamic S-box design based on combined chaotic map and fitness function," *Multimedia Tools and Applications*, vol. 79, pp. 12329–12347, 2020, doi: 10.1007/s11042-019-08478-0.

BIOGRAPHIES OF AUTHORS

Huda Rashid Shakir received a B.Sc. in Computer Sciences from Mustansiriyah University, Baghdad, Iraq. Currently, she is studying M. Sc. in Computer Science, College of Education, Department of Computer Science, Mustansiriya University, as well as working in the Iraqi Ministry of Education. She can be contacted at email: hudarashid@uomustansiriyah.edu.iq.

Sadiq Abdul Aziz Mehdi received the B.Sc. in Mathematical Sciences from Mustansiriyah University, Baghdad, Iraq in 1996, M.Sc. in Applied Mathematics Sciences-Modeling and Simulation from Al al-Bayt University, Jordan in 2002, and Ph.D. in Applied Mathematics/Data Cryptography from University of Mustansiriyah, Baghdad, Iraq in 2011. Current position & Functions: computer science from Mustansiriyah University. His research interest is in the fields of Dynamical system, Chaotic system, Chaotic Encryption and Modeling & Simulation. He can be contacted at email: sadiqmehdi71@uomustansiriyah.edu.iq.

Anwar Abbas Hattab received the B.Sc in Computer Science from Baghdad University and her MSc degree in Network Management in 2003 from the Iraq Commission for Computer and Informatics, Institute for Post Graduate Studies in Informatics. Currently she is a lecturer in computer science. Anwar has more than 18 years of experience and has supervised Msc and BSc final year project. Her research interests include cryptography, image processing, data security, network security, and databases. She can be contacted at email: anwarabbas76@uomustansiriyah.edu.iq.