Received: May 19, 2022. Revised: June 30, 2022. 378

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Creation of S-Box based One-Dimensional Chaotic Logistic Map: Colour Image Encryption Approach

Rasool S. Salman[1]* Alaa K. Farhan[2] Ali Shakir[1]

[1]*Department of Computer Sciences, University of Mustansiriyah, Baghdad, Iraq*
[2]*Department of Computer Sciences, University of Technology, Baghdad, Iraq*
* Corresponding author's Email: rasoulsalah@uomustansiriyah.edu.iq

Abstract: Image security is evolving as an outstanding platform to provide security in the digital world. The external features of the Internet have driven the transfer of digital images from one place to another. In the area of security, the improvement of encryption and decryption is crucial. Chaos-based encryption has recently been proposed as a reliable and effective solution for image security. The excellent properties of unpredictability, ergodicity, and sensitivity to their parameters and initial values have enabled the wide use of chaotic maps in security applications. This paper introduces a colour image encryption approach to secure colour images and constructs s-box relying on the one-dimensional logistic map. The proposed colour image encryption approach relies on the generated new S-box. The new S-box passed the S-box test criteria for balanced, completeness, avalanche, and strict avalanche. Also, the encryption performance analysis metrics like information entropy, correlation analysis, histogram analysis, and differential attack are recorded. Based on the results, the values of information entropy, NPCR, and UACI for the Lena image reached are 7.9972, 99.601%, and 33.5647% respectively.

Keywords: Colour image encryption, Chaotic maps, New S-box, Logistic map, RGB.

1. Introduction

The development of network communication has led to a rise in the need for different types of cryptographic systems to protect information that is transmitted through the networks [1]. One of the most essential types of information transmitted through the internet is multimedia information, which includes colour images, videos, and audio. How to convey this information securely has become an essential issue. Thus, digital image encryption is one of the most active research areas in cryptography [2]. In recent years, the majority of studies have focused on gray and colour images Colour images contain more information than gray images and are therefore more attractive [3]. Many researchers have introduced several techniques to protect colour images, such as hyper chaos and Genetic Codes [4], Rubik's Cube [5], DNA [6], henon-zigzag map [7], Cellular Neural Network [8], genetic algorithm and matrix semi-tensor product [9], Lorenz equation and Gingerbreadman chaotic map [10], chaotic cipher [11], amplitude-phase encoding and discrete complex random transformation [12], mixed hash functions and cyclic shift [13] and chaos-based probabilistic symmetric encryption [14]. DES and AES are also used to encrypt images as modern cryptographic algorithms [15], but they are not appropriate for images due to the image's physical properties such as large data, robust correlations between pixels, and high redundancy.

Chaotic maps are dynamic models with excellent features such as unpredictable, periodic behaviour and sensitivity to system parameters as well as sensitivity to initial values. There are two classes of chaotic maps: one-dimensional(1-D) [16] and multi-dimensional(M-D) [17]. Most one-dimensional chaotic maps, like the Logistic, Piecewise linear, and Tent map [18], are made up of one variable and a few parameters.

Substitution box (S-box) is the non-linear operation involved in most block ciphers [19]. to give

block ciphers more secure, many researchers focused on creating robust S-Boxes relied on chaos systems. In 2012, M. Khan et al. [20] designed a new S-Box based on the Lorenz system. Their proposed S-Box was evaluated by the criteria of strict avalanche, linear approximation, differential approximation, bit independence, and non-linearity. In 2016, B. K. Maram and J. M. Gnanasekar [21] presented a strong S-Box based on a pseudo-random number generator and public key. The proposed S-Box tests showed good results when tested with S-box parameters such as Balanced Criteria, Hamming Distance, and Avalanche Effect and can be used with cryptographic algorithms. In 2017, Dragan Lambic [22] suggested a new approach for the creation of s-box relied on a discrete logistic map. His proposed evaluated by utilizing S-Box criteria, and the outcomes show the suggested s-box has good encryption properties. In 2016, A. Alzaidi et al. [18] proposed a new method for the construction of S-Box based on an enhanced 1-D chaotic map and B-hill climbing search. The proposed method was tested with some S-Box parameters, and the results showed that the generated S-Box has a good security level and is found to be better when compared with related S-Boxes. In 2019, Q. Lu et al. [23] proposed a new algorithm to generate S-Boxes relying on compounds (chaotic systems and ten-logistic map) (TLS). Firstly, they generated the initial S-Box by using new linear mapping and then scrambled it by the TLS. The generated S-Boxes have higher scores in linear probability and differential probability than other S-Boxes. In 2021, G. Hanchinamani et al [24] provided a new approach of creating Sbox relying on mixing the variables of chaotic maps. Their presented S-Box satisfied the S-Box criteria and was found to be better as compared with other approaches. In 2021, M. Fadhil et al. [25] presented a new S-Box by using a one-dimentional logistic map. Firstly, they converted the output values of chaiotic to hex values and then generated the new S-box. The proposed S-Box satisfied the standard S-box criteria. Also, the researchers in [26-28] used chaotic systems in order to design robust S-Boxes.

In this paper, we present two proposals. The first proposal is to create S-Box (16X16) relied on a 1-dimensional logistic map to increase its nonlinearity. The second proposal is to design a new scheme to encrypt colour images and make it very suitable to deal with the image's physical properties such as large data, robust correlations between pixels, and high redundancy , which involves separating the colour image into three channels, R, G, and B, and rotating them using a 180-degree rotation operation and confusing the three channels using the new S-Box. Furthermore, the new S-box meets the S-box test criteria for balanced, completeness, avalanche, and strict avalanche. Also, the images that were encrypted by using the new S-box achieved good results in terms of entropy, correlation, and differential attack.

The following were our contributions:

a- A 1-dimensional chaotic logistic map is utilized to construct a robust S-Box.
b- presenting a new method to encrypt colour images based on the generated new S-Box.
c- evaluating the new S-box with S-Box evaluation criteria including balanced, completeness, avalanche, and strict avalanche.
d- evaluating the new colour image encryption scheme with some metrics such as entropy, correlation, and differential attacks.

The remainder of the article is structured as follows: Section 2 illustrates the choice theory and explains the 1-dimensional logistic map. Section 3 offers two proposed methods to generate S-Box and encrypt colour images. Section 4 discusses the results of these two proposals. The Section 5 contains the conclusion.

2. Chaos theory

Chaotic is an aperiodic, long-term behaviour that appears in a deterministic system [29]. Chaos-based systems are extremely sensitive to initial conditions called the "butterfly effect" [30]. Nonlinear dynamical discrete time systems that show chaotic behaviour are called "chaotic maps." The advantage of a chaotic map is that it is deterministic. Many researchers take this advantage of a chaotic system and use it with the good properties of cypher cryptography like confusion and diffusion to increase the security [31, 32]. The chaos system can be used for systems that need security, such as image encryption algorithms, block and stream ciphers, etc. [33]. There are different chaotic systems seen in Table 1 of which the logistic map is commonly used [34].

One-dimensional logistic map is simple and are capable of exhibiting chaotic behaviour. Generally, the one-dimensional logistic maps can be represented mathematically as Eq. (1) [23, 35].

$$xi + 1 = \varphi x_i (1 - x_i) \quad (1)$$

Where x0 $\in$ (0,1) represent the initial state at any time i, φ is a control parameter $\in$ (0 ,4), and (Xi+1) is the next state of the system, Fig. 1 shows how the x value changes over iterations. The x behaves differently based on the φ value as in Fig. 2 [31]. In

Table 1. Type of chaotic maps [34]

Maps name	Domain	Dimension
Logistic	Discrete	1
Piecewise linear chaotic	Discrete	1
Tent	Discrete	1
Gaussian	Discrete	1
Cat	Discrete	2
Baker	Discrete	2
Standard	Discrete	2
Jerk equation	Continuous	3
Roster	Continuous	3
Chen	Continuous	3
Lorenz	Continuous	3

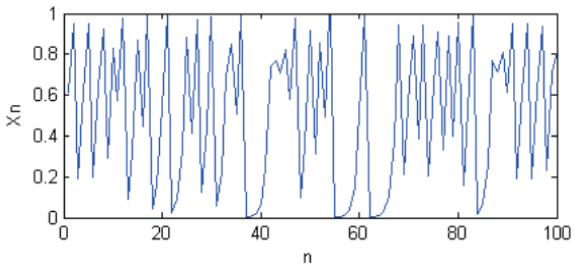

Figure. 1 The logistic chaotic behaviour with iteration values [36]

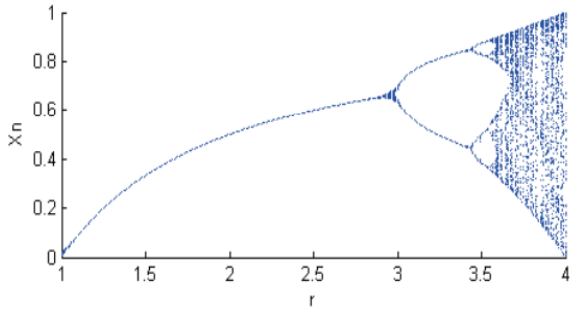

Figure. 2 Changes of x value based on the r (φ) value [36]

this paper, we used the one-dimensional logistics map to build the s-box.

3. Research methods

This research introduces a new approach for constructing S-box, which is the source of confusion in block ciphers, and also introduces a new scheme to encrypt colour images by using the new S-box with some operations such as rotating to achieve diffusion. Since chaos systems and cryptography are very compatible, we relied on the 1D logistic map to generate this S-Box, as illustrated in Fig. 3. The generation of s-box is done as follows: First, generating a hex code relied on a 1-D logistic map, and then constructing the new s-box from the generated hex code, as illustrated by algorithm 1. Algorithm 2 illustrates the process of constructing an inverse S-Box. As shown in Fig. 4, after generating the new S-Box, we use it to encrypt the colour image with our proposed encryption scheme.

3.1 Process of constructing the new S-Box and inverse S-Box

The new S-box is generated as follows: (1) reading the input initial condition parameters φ and xi, (2) computing the xi value and converting it to hex code, getting only the two digits that start from digit 7 to 9, and then storing it in a 16x16 array while checking that the values are not repeated. We repeat step 2 until we get 256 values, which represents the generated s-box matrix that can be utilized in the encryption. Algorithm 1 represents S-Box generation.

Algorithm 2 represents the steps that are needed to construct the inverse of the generated S-Box, which is needed in the decryption process to get the original data.

3.2 Process of color image encryption

After generating the new S-Box, we utilize the suggested colour image encryption approach to encrypt the colour image as shown in Fig. 4 and as follows: (1) separating the colour image into its colour channels (CH-R, CH-G, and CH-B). (2)

Algorithm 1: Generating S-Box using 1D chaotic logistic map

Input: initial values(φ and *x*0) for the 1-D logistic map
Output: New S-Box 8X8
Begin:
Step 1: read initial conditions
Step 2: Set i= 0, index= 0, float X array= Null, string H = Null, string S array= Null, string array S-Box [16,16]
Step 3: While (i < 256)
Step 3.1: x [i + 1] = φ * x[i] * (1 - x[i])
Step 3.2: Convert x[i] to hex and get only two digits from index (7 to 9) and then save it in H
Step 3.3: If (S contents H) Then i++ and go to step 3} // This step is to avoid duplication of values
Step 3.4: else s[i]=H; i++ and go to step 3
Step 3.5: End if
Step 4: End While
Step 5; For i=0 to 15
Step 5.1: For j=0 to 15
Step 5.2: S-Box [i, j] = S[index]
Step 5.3: index ++
Step 5.4: next j
Step 6: next i
Step 7: End for
Step8: End for
End

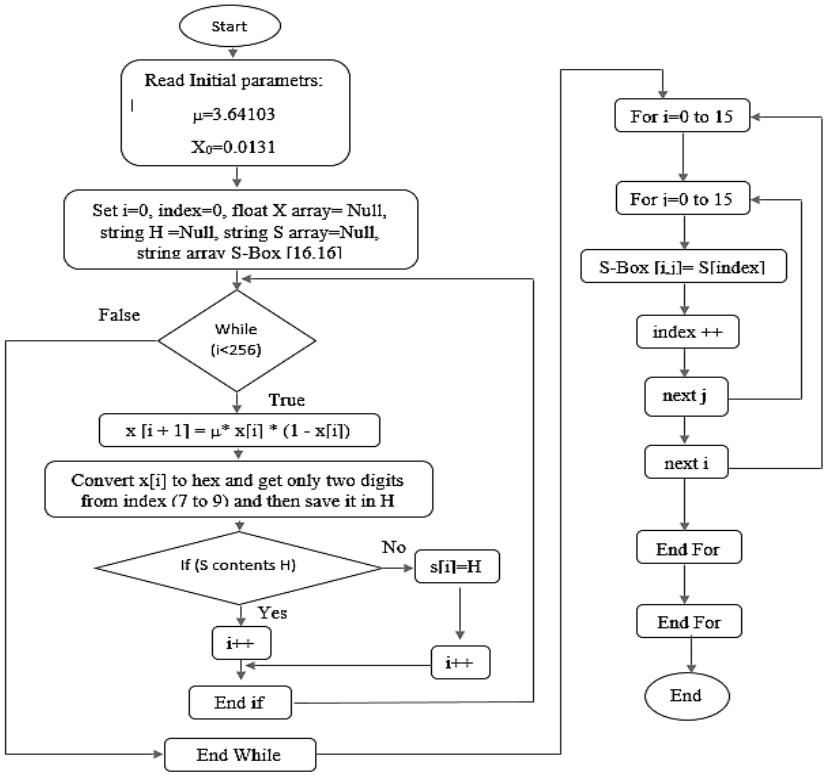

Figure. 3 Flow chart of construct new S-box

Algorithm 2: Inverse the generated S-Box

Input: S-Box generated from algorithm 1
Output: invers S-Box 16X16
Begin:
Step 1: set a=0, b=0, string array Inv-Sbox [16,16] = Null
Step 2: For i=0 to 15
Step 2.1: for j=0 to 15
Step 2.2: get first digit from S-Box [I, j] and convert it to Integer and save it in a
Step 2.3: get second digit from S-Box [I, j] and convert it to Integer and save it in b
Step 2.4: convert I and j to hex and CONCATENATE them and the save them in the Inv-Sbox [a, b]
Step 2.5: next j
Step3: next i
Step 4: end for
Step 5: end for
End

rotating the positions of each channel's values by 180 degrees to create the diffusion effect as shown in Fig. 5. (3) Applying the new s-box to each channel to add the confusion effect. (4) swapping rows with columns for each channel to increase diffusion. (5) performing a xor operation on the values of rows CH-R and CH-G to generate new CH-G values. (6) performing a xor operation on the values of columns CH-B and the new CH-G to generate new CH-G values. (7) Applying the xor operation between the values of the CH-R's rows and the values of the columns of the new CH-G to produce a new CH-R and, at the same time, applying the xor operation between the values of the CH-B's rows and the values of the columns of the new CH-G to produce a new CH-B. (8) Shifting the positions of the values of pixels in each channel (new CH-R, new CH-G, and new CH-B) by traversal it Diagonally as shown in Fig. 6 that is for more diffusion. (9) combining the channels that were obtained from step 8 to produce the encrypted image. The decryption is invers process. Decryption is the opposite of the above operations, but with the use of the inverse of the S-box.

4. Results and discussion

The generation of the S-box and its inverse took just 6 Ms, which was measured by the Visual Studio 2017 C#. Furthermore, the new S-box meets the S-box test criteria for balanced, completeness, avalanche, and strict avalanche. Also, the images that were encrypted by using the generated S-box achieved good results in terms of entropy, correlation, histogram analysis, and differential attack. Below, we explain all of the S-box criteria and image encryption metrics. All of the results were compared to related works.

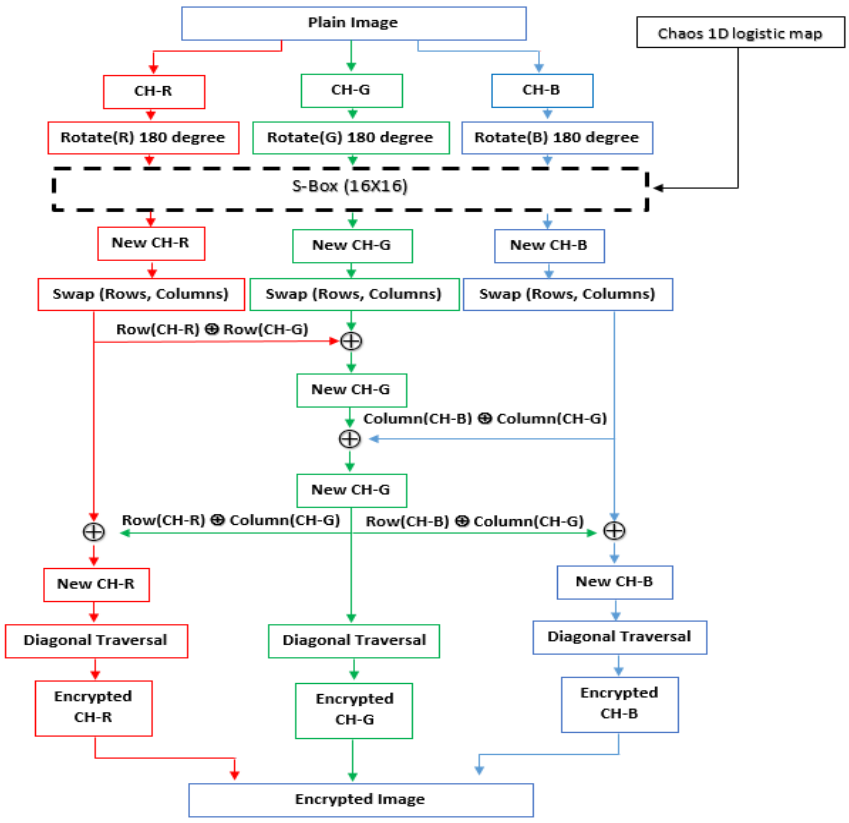

Figure. 4 The suggested colour image encryption scheme

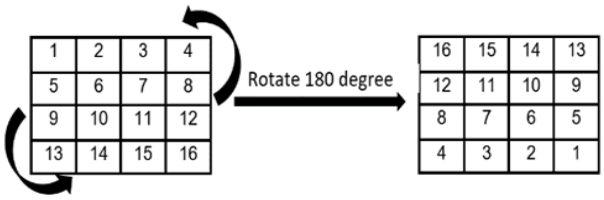

Figure. 5 Rotate matrix 180 degree

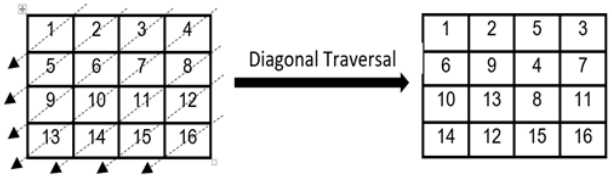

Figure. 6 Matrix traversal diagonally

Table 2. Compared the new S-box BC test to related S-boxes

Method	Words			
	"Computer"		"ABMNOPQR"	
	0's	1's	0's	1's
[18]	34	30	27	37
[20]	39	25	30	34
[21]	33	31	31	33
[22]	30	34	38	26
[23]	35	29	28	36
[24]	28	36	40	24
[25]	32	32	33	31
Proposed S-box	**32**	**32**	**32**	**32**

4.1 S-Box criteria

4.1.1. Balanced criterion (BC)

One of the most important S-Box tests is to check the distribution of the 0's and 1's in the output sequences, which must be balanced [21, 37]. This test used two words with the new S-box and the results show that the new S-box is balanced because it has an equal number of 0's and 1's, as shown in Table 2.

Fig. 7 and 8 show the BC test on the new s-box and the s-boxes for related work. Where Fig. 7 shows the number of zeros and ones for the string "Computer" after changing it with new data from s-box, Fig. 8 shows the number of 0's and 1's for the string "ABMNOPQR", also after changing it with new s-box data.

4.1.2. The completeness criterion (CC)

This criterion determines completeness, which indicates that every bit of the output is subjected to all of the input bits [38]. For the produced S-box, Table 3 to 6 illustrate that the generated S-box satisfies this test because every bit of the output of produced S-boxes depends on the whole input bits (initial conditions φ and $x0$).

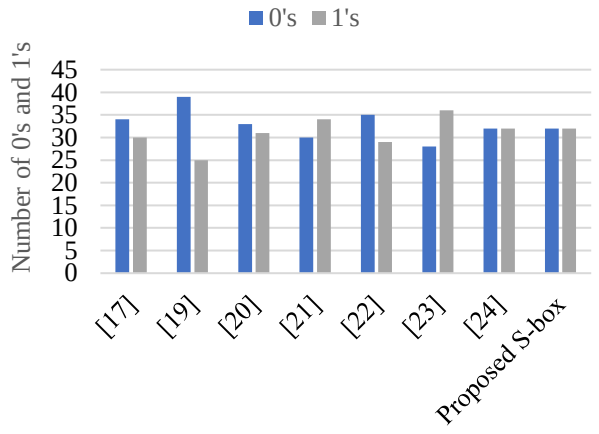

Figure. 7 BC test on the output of the generated S-box for the string "computer" and compared with previous similar studies

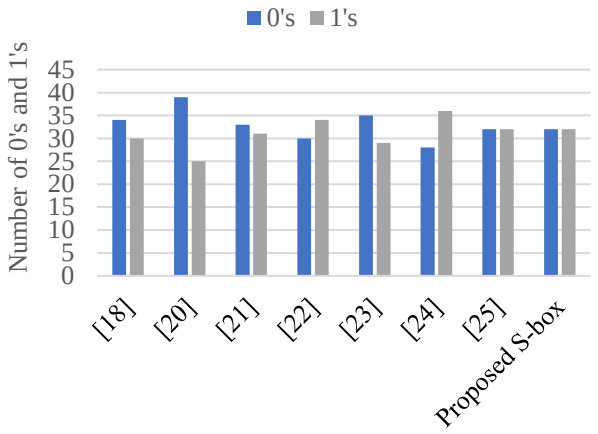

Figure. 8 BC test on the output of the generated S-box for the string "ABMNOPQR" and compared with previous similar studies

Table 3. S-box generated by using the inputs u=3.64103 and x0= 0.0131

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

Table 4. Invers S-box when inputs u=3.64103 and x0= 0.0131

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

Table 5. S-box generated by using the inputs u=3.64103 and x0= 0.00131

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

Table 6. Invers S-box when inputs u=3.64103 and x0= 0.00131

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

4.1.3. Avalanche criteria (AC)

The non-relationship between input bits and output sequence is an important and desirable feature of a good block cipher, which is evaluated using the avalanche criterion, meaning that a slight alteration in plaintext results to a big alteration in ciphertext, like a flipping single bit from 0 to 1 or inversely, leading to a large alteration in the output. The value of this criterion is calculated using Eq. (2) and should be within the range of (0–1), where the optimal value equals to 0.5, which indicates it satisfies the avalanche criterion [38]. Table 7 shows AC test.

$$AC = \frac{Number\ of\ Flipped\ Bits\ in\ Cipher\ Text}{Number\ of\ All\ Bits\ in\ Cipher\ Text} \quad (2)$$

To evaluate the proposed S-box, we flipped single bit from the letter "L" to become "M" and replaced both "L" and "M" with other data from the proposed S-box. The result of "L" was different than "M" in 5 bits out of the original 8 bits. As a result of Eq. (2), the AC equals 0.625, which means the generated S-box fulfils the avalanche criterion. The outcomes of this test were compared with other results of related studies, as shown in Table 7 and Fig. 9.

4.1.4. Strict avalanche criterion (SAC)

When flipping one bit from the input causes a change of 50% in the output bits, the S-box fulfils the SAC [39, 40]. The SAC is achieved when both AC

Table 7. Compared the new S-box AC test to related S-Boxes

Method	Original Data	Binary input	Binary output	Avalanche Criteria
[18] Flipping one bit	L	01001100	01101101	4/8=0.5
	M	01001101	01011011	
[20] Flipping one bit	L	01001100	10000100	4/8 =0.5
	M	01001101	00100111	
[21] Flipping one bit	L	01001100	11011011	4/8=0.5
	M	01001101	01000001	
[22] Flipping one bit	L	01001100	01111000	5/8=0.625
	M	01001101	01011100	
[23] Flipping one bit	L	01001100	10111110	3/8 =0.375
	M	01001101	01111111	
[24] Flipping one bit	L	01001100	10010001	3/8=0.375
	M	01001101	01000001	
[25] Flipping one bit	L	01001100	00010100	5/8 =0.625
	M	01001101	10000011	
Proposed S-box Flipping one bit	L	01001100	11001011	5/8 =0.625
	M	01001101	00010111	

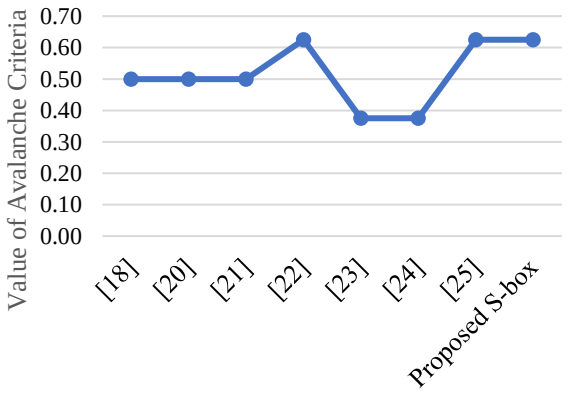

Figure. 9 AC test for the new S-box and comparison with previous similar studies

and CC are achieved together [41, 42]. Therefore, since our proposal fulfils the criteria AC and CC, it fulfils the SAC.

4.2 Image encryption metrics

4.2.1. Entropy

Entropy is defined as the measurement of the randomness of the data within an image. If the value of the entropy is high, it means the data within the image is more disordered [43, 44]. Eq. (3) is utilized to measure the entropy. the entropy value should be close or equal to 8 [45].

Table 8. Information entropy results with comparison to related works

method	image	Entropy (Average)
Our proposed	Lena	7.9972
	Baboon	7.9978
	Woman	7.9821
	Peppers	7.9966
[9]	Lena	7.9972
[10]	Peppers	7.9959
[11]	Lena	7.9943

Table 9. Results of correlation coefficients

image	Correlation (Average)
Lena	0.00193
Baboon	-0.002810
Woman	0.002129
Peppers	0.00304

$$Entropy = \sum_i P(s_i) Log2 \left(\frac{1}{P(s_i)}\right) \quad (3)$$

Where P (s_i) represents the probability of pixel s_i (i=0 to 255) in an image.

From Table 8, it is shown that the entropy value is closer to 8. The probability of accidental information leakage is very less if it is very close to 8. The proposed scheme is better than [10] and [11] studies.

4.2.2. Correlation analysis

It is defined as the relationship between the pixels that make up the actual image and the pixels that make up the encrypted image. Based on the correlation, the similarity between the actual image and the encrypted image will be evaluated. For a best encryption process, there must be a low correlation. [46]. Eq. (4) represent the correlation mathematically.

$$Correlation = \sum \left(\frac{(i-\mu i)(j-\mu j)}{\sigma_i \sigma_j}\right) \quad (4)$$

From Table 9, the correlation values in every direction of the four images are close to 0, i.e. no correlation seems in the neighbour pixels in the four encrypted images.

4.2.3. Histogram analysis

A histogram indicates the frequent appearances of colour values in cipher images and plain images.

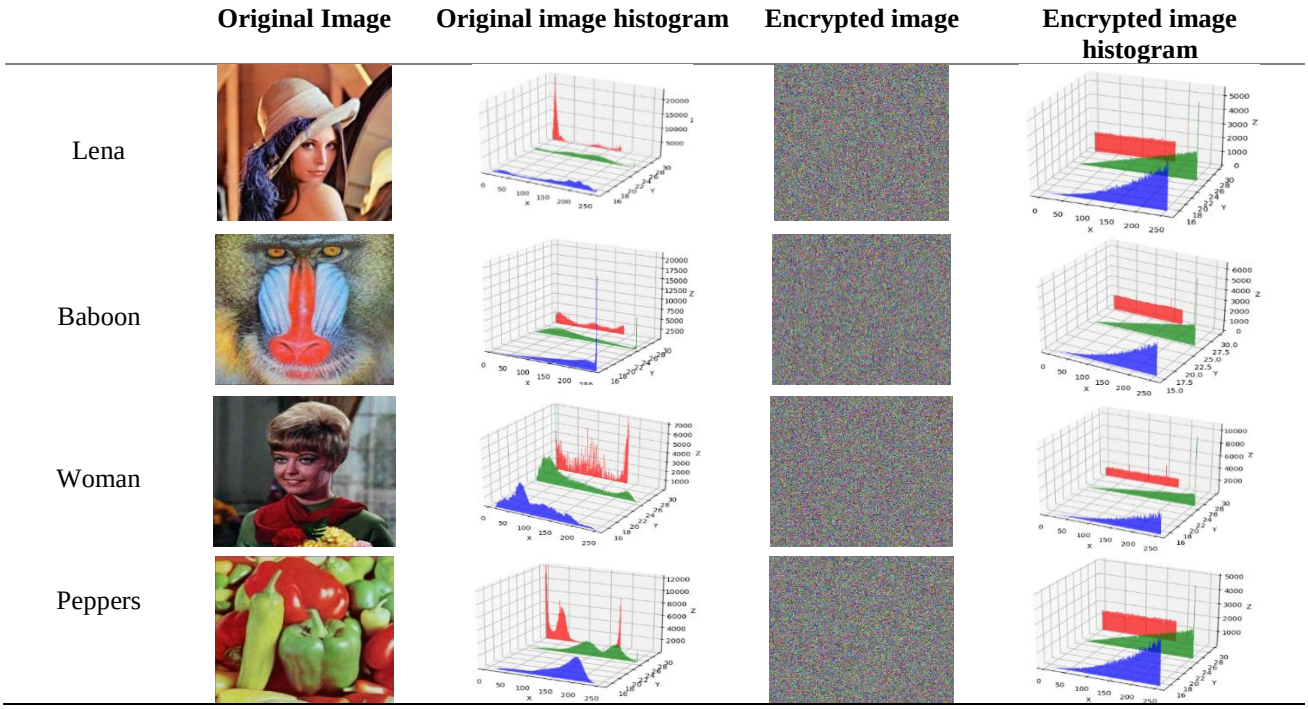

Figure. 10 Histogram analysis

The cipher image histogram is widely uniform and flat in distribution [9, 45, 47]. Because the histograms of plain images vary, the attacker usually makes use of this statistical property to break the cipher. To avoid this danger, the cipher must remove the statistical property of the plain image during encryption. The histograms of the four plain, encrypted, and decrypted images are shown in Fig (10). The visual comparison makes it clear that the cipher image histograms are almost flat. So, it can be said that statistical attacks don't give the attacker any useful information.

4.2.4. Differential attack

suggested image encryption approach has been analysed for differential attack on four images utilizing two metrics - number of pixel change rate (NPCR) and unified average change intensity (UACI) which are specified for a M×H image size utilizing Eqs. (5) and (6).

$$NPCR = \left[\frac{\sum_{i,j} I(i,j)}{M \times H}\right].100\% \qquad (5)\ [48]$$

$$UACI = \frac{1}{M \times H}\left[\frac{\sum_{i,j}|C(i,j)-C'(i,j)|}{255}\right].100\% \ (6)\ [46]$$

Where I (i, j) = 1 if C (i, j) ≠C' (i, j), otherwise I (i, j) =0 and C and C' indicate the encrypted images of actual image before and after one-pixel alteration in the actual image [49, 50]. For analysis, one pixel of input image has been changed to get the encrypted image C'. The outcomes of NPCR and UACI for the four images are listed in Table 10 with compare to related works.

Table 10. NPCR and UAC values with comparison to related works

method	image	Average $NPCR_{R,G,B}$ (%)	Average UACI $_{R,G,B}$ (%)
Our proposed	Lena	99.601	33.5647
	Baboon	99.604	33.5662
	Woman	99.557	33.7107
	Peppers	99.594	33.5772
[12]	Lena	99.581	33.6665
[13]	Lena	99.595	33.5512
[14]	Lena	99.580	33.5008

From the Table 10 it is noticed that the suggested scheme is delicate to alter one-pixel and it is best than the [12, 13, 14] studies.

5. Conclusion

A colour image encryption approach with a diffusion and permutation mechanism by using the proposed new S-box that is constructed relying on a 1-D logistic map was suggested in this paper. The generated SBox passed the balanced, completeness, avalanche, and strict avalanche criteria for the test S-box. This indicates that the proposed SBox has good properties for encryption. it was built in only 7 milliseconds, which can be utilized in the advanced encryption standard(AES) and other lightweight algorithms. The proposed colour image encryption

system also improves correlation, entropy level, and establishes a uniform distribution of histogram and differential attack analysis. The values of information entropy, NPCR, and UACI for the Lena image reached are 7.9972, 99.601%, and 33.5647%, respectively, which are higher than cited related works. From these results, it is observed that the information entropy is close to 8, the NPCR > 99.6% and the UACI > 33.4. This indicates that the proposed colour image encryption approach has more security. In future work, we can combine the logistic map with another type of chaos system to make an S-Box with a higher level of security.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The first author was responsible for methodology, software, validation, formal analysis, investigation, resources, data curation, writing original draft preparation, writing review and editing, and visualization, while the authors second and third were responsible for supervision and project administration.

References

[1] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review", *J. Inf. Secur. Appl.*, Vol. 48, p. 102361, 2019, doi: 10.1016/j.jisa.2019.102361.

[2] S. Zhou, X. Wang, M. Wang, and Y. Zhang, "Simple colour image cryptosystem with very high level of security", *Chaos, Solitons and Fractals*, Vol. 141, p. 110225, 2020, doi: 10.1016/j.chaos.2020.110225.

[3] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images", *Signal Processing*, Vol. 164, pp. 163-185, 2019, doi: 10.1016/j.sigpro.2019.06.010.

[4] H. Nazir, I. S. Bajwa, S. Abdullah, R. Kazmi, and M. Samiullah, "A Color Image Encryption Scheme Combining Hyperchaos and Genetic Codes", *IEEE Access*, Vol. 10, pp. 14480-14495, 2022, doi: 10.1109/ACCESS.2022.3143096.

[5] J. Zhao, J. Zhao, T. Zhang, J. Jiang, T. Fang, and H. Ma, "Color Image Encryption Scheme Based On Alternate Quantum Walk and Controlled Rubik's Cube", *IOSR J. Math.*, Vol. 18, No. 4, pp. 16–25, 2022, doi: 10.9790/5728-1804011625.

[6] I. A. Aljazaery, H. T. S. Alrikabi, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor", *Int. J. online Biomed. Eng.*, Vol. 18, No. 3, pp. 101-113, 2022, doi: 10.3991/ijoe.v18i03.28021.

[7] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain", *Opt. Laser Technol.*, Vol. 135, No. October 2020, p. 106610, 2021, doi: 10.1016/j.optlastec.2020.106610.

[8] R. Zhang, L. Yu, D. Jiang, W. Ding, J. Song, K. He, and Q. Ding, "A novel plaintext-related color image encryption scheme based on cellular neural network and chen's chaotic system", *Symmetry (Basel).*, Vol. 13, No. 3, pp. 1-19, 2021, doi: 10.3390/sym13030393.

[9] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption", *Signal Processing*, Vol. 183, p. 108041, 2021, doi: 10.1016/j.sigpro.2021.108041.

[10] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S 8 permutation", *J. Intell. Fuzzy Syst.*, Vol. 33, No. 6, pp. 3753-3765, 2017, doi: 10.3233/JIFS-17656.

[11] J. Thiyagarajan, B. Murugan, and A. G. N. Gounder, "A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity", *Serbian J. Electr. Eng.*, Vol. 16, No. 2, pp. 247-265, 2019, doi: 10.2298/SJEE1902247T.

[12] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, "A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation", *IEEE Access*, Vol. 6, No. c, pp. 77740-77753, 2018, doi: 10.1109/ACCESS.2018.2884013.

[13] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift", *Opt. Lasers Eng.*, Vol. 107, No. December 2016, pp. 370-379, 2018, doi: 10.1016/j.optlaseng.2017.06.015.

[14] S. Dhall, S. K. Pal, and K. Sharma, "A chaos-based probabilistic block cipher for image encryption", *J. King Saud Univ. - Comput. Inf. Sci.*, Vol. 34, No. 1, pp. 1533-1543, 2018, doi: 10.1016/j.jksuci.2018.09.015.

[15] B. Harjo and D. Setiadi, "Improved Color Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method Improved Color Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method", *Int. J. Intell. Eng. Syst.*, Vol. 14, No. 2, 2021, doi:

10.22266/ijies2021.0430.14, doi: 10.22266/ijies2021.0430.14.

[16] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map", *Signal Processing*, Vol. 138, pp. 129-137, 2017, doi: 10.1016/j.sigpro.2017.03.011.

[17] A. D. I. Alhudhaif, M. Ahmad, A. Alkhayyat, A. K. Farhan, and R. Ahmed, "Block Cipher Nonlinear Confusion Components Based on New 5-D Hyperchaotic System", *IEEE Access*, Vol. 9, pp. 87686-87696, 2021, doi: 10.1109/ACCESS.2021.3090163.

[18] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes", *IEEE Access*, Vol. 6, pp. 55405-55418, 2018, doi: 10.1109/ACCESS.2018.2871557.

[19] M. S. M. Malik, M. A. Ali, M. A. Khan, M. E. U. Haq, S. N. M. Shah, M. Rehman, and W. Ahmad, "Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices", *IEEE Access*, Vol. 8, pp. 35682-35695, 2020, doi: 10.1109/ACCESS.2020.2973679.

[20] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems", *Nonlinear Dyn.*, Vol. 70, No. 3, pp. 2303-2311, 2012, doi: 10.1007/s11071-012-0621-x.

[21] B. K. Maram 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.

[22] D. Lambić, "A novel method of S-box design based on discrete chaotic map", *Nonlinear Dyn.*, Vol. 87, No. 4, pp. 2407-2413, 2017, doi: 10.1007/s11071-016-3199-x.

[23] Q. Lu, C. Zhu, and G. Wang, "A Novel S-Box Design Algorithm Based on a New Compound Chaotic System", *Entropy Artic.*, pp. 1-15, 2019.

[24] G. Hanchinamani, D. G. Narayan, and R. Savakknavar, "Construction of S-box based on parametric mixing of chaotic maps", In: *Proc. of the 2021 1st International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies, ICAECT 2021*, No. 1, 2021, doi: 10.1109/ICAECT49130.2021.9392537.

[25] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, "Designing Substitution Box Based on the 1D Logistic Map Chaotic System", In: *Proc. of 2nd International Scientific Conference of Engineering Sciences*, Vol. 1076, No. Isces 2020, pp. 1-12, 2021, doi: 10.1088/1757-899X/1076/1/012041.

[26] M. Ahmad, E. A. Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures", *IEEE Access*, Vol. 8, pp. 110397-110411, 2020, doi: 10.1109/ACCESS.2020.3001868.

[27] A. A. A. E. Latif, B. A. El-atty, A. Belazi, and A. M. Iliyasu, "Efficient chaos-based substitution-box and its application to image encryption", *Electron.*, Vol. 10, No. 12, pp. 1-19, 2021, doi: 10.3390/electronics10121392.

[28] S. A. Jassim and A. K. Farhan, "Designing a Novel Efficient Substitution-Box by Using a Flower Pollination Algorithm and Chaos System", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 1, pp. 176–187, 2022, doi: 10.22266/IJIES2022.0228.17.

[29] A. Kadhim and H. Emad, "Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers", *Diyala J. Pure Sci.*, Vol. 13, No. 3, pp. 24-39, 2017, doi: 10.24237/djps.1303.268b.

[30] H. Natiq, N. M. G. A. Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption", *Eur. Phys. J. Plus*, Vol. 133, No. 1, 2018, doi: 10.1140/epjp/i2018-11834-2.

[31] A. Abdulgader, M. Ismail, N. Zainal, and T. Idbeaa, "Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption", *J. Theor. Appl. Inf. Technol.*, Vol. 71, No. 1, pp. 1-12, 2015.

[32] Y. Q. Zhang, J. L. Hao, and X. Y. Wang, "An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map", *IEEE Access*, Vol. 8, pp. 54175-54188, 2020, doi: 10.1109/ACCESS.2020.2979827.

[33] O. Jallouli, "Chaos-based security under real-time and energy To cite this version : Thèse de Doctorat Ons J ALLOULI", 2017.

[34] A. Kadhim and R. S. Ali, "Enhancement AES based on 3D chaos theory and DNA operations addition", *Karbala Int. J. Mod. Sci.*, Vol. 5, No. 2, 2019, doi: 10.33640/2405-609X.1137.

[35] A. T. Sadiq, A. K. Farhan, and S. A. Hassan, "A PROPOSAL TO IMPROVE RC4 ALGORITHM BASED ON HYBRID CHAOTIC MAPS", *J. Adv. Comput. Sci. Technol. Res.*, Vol. 6, No. 4, pp. 74-81, 2016.

[36] N. Hazarika and M. Saikia, "A novel partial image encryption using chaotic logistic map",

In: *Proc. of 2014 International Conference on Signal Processing and Integrated Networks, SPIN 2014*, pp. 231-236, 2014, doi: 10.1109/spin.2014.6776953.

[37] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle Swarm Optimization Based Highly Nonlinear Substitution-Boxes Generation for Security Applications", *IEEE Access*, Vol. 8, pp. 116132-116147, 2020, doi: 10.1109/ACCESS.2020.3004449.

[38] I. Journal and S. Sciences, "A Review of Block Cipher's S-Boxes Tests Criteria", *Iraqi J. Stat. Sci.*, No. 19, pp. 39-48, 2019.

[39] E. Tanyildizi and F. Ozkaynak, "A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps", *IEEE Access*, Vol. 7, pp. 117829-117838, 2019, doi: 10.1109/ACCESS.2019.2936447.

[40] A. H. Zahid, E. A. Solami, and M. Ahmad, "A Novel Modular Approach Based Substitution-Box Design for Image Encryption", *IEEE Access*, Vol. 8, pp. 150326-150340, 2020, doi: 10.1109/ACCESS.2020.3016401.

[41] A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. A. Saidi, and G. H. A. Majeed, "A new approach to generate multi S-boxes based on RNA computing", *Int. J. Innov. Comput. Inf. Control*, Vol. 16, No. 1, pp. 331-348, 2020, doi: 10.24507/ijicic.16.01.331.

[42] N. B. Abdulwahed, "CHAOS-BASED ADVANCED ENCRYPTION STANDARD Thesis by Naif B . Abdulwahed In Partial Fulfillment of the Requirements for the degree of Master of Science", 2013.

[43] A. Kadhim and R. M. Mohamed, "Visual cryptography for image depend on RSA & AlGamal algorithms", In: *Proc. of Al-Sadiq International Conference on Multidisciplinary in IT and Communication Techniques Science and Applications, AIC-MITCSA 2016*, pp. 195-200, 2016, doi: 10.1109/AIC-MITCSA.2016.7759935.

[44] Y. Naseer, T. Shah, S. Hussain, and A. Ali, "Steps Towards Redesigning Cryptosystems by a Non-associative Algebra of IP-Loops", *Wirel. Pers. Commun.*, Vol. 108, No. 3, pp. 1379-1392, 2019, doi: 10.1007/s11277-019-06474-z.

[45] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy", *Signal Processing*, Vol. 176, p. 107684, 2020, doi: 10.1016/j.sigpro.2020.107684.

[46] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications", *Chinese J. Phys.*, Vol. 56, No. 4, pp. 1609-1621, 2018, doi: 10.1016/j.cjph.2018.04.013.

[47] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos", *Signal Processing*, Vol. 155, pp. 44-62, 2018, doi: 10.1016/j.sigpro.2018.09.029.

[48] M. Yildirim, "A color image encryption scheme reducing the correlations between R, G, B components", *Optik (Stuttg).*, Vol. 237, No. March, p. 166728, 2021, doi: 10.1016/j.ijleo.2021.166728.

[49] M. Yildirim, "DNA encoding for RGB image encryption with memristor based neuron model and chaos phenomenon", *Microelectronics J.*, Vol. 104, No. March, p. 104878, 2020, doi: 10.1016/j.mejo.2020.104878.

[50] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map", *Opt. Lasers Eng.*, Vol. 121, No. November 2018, pp. 203-214, 2019, doi: 10.1016/j.optlaseng.2019.04.011.