Received: July 14, 2023. Revised: September 9, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Generation of Dynamic Substitution Boxes Using HSM Chaos System for Application in Color Images Encrypting

Sura Mazin Ali[1] **Alyaa hasan zwiad**[2] **Rusul Mansoor Al-Amri**[3] **Alaa Kadhim Farhan**[2]*

[1]*Political Science College, Al Mustansiriyah University, Baghdad 10052, Iraq*
[2]*Computer Science Department, University of Technology, Baghdad 10066, Iraq*
[3]*College of Nursing, University of Al-Ameed ,Karbala 198,Iraq*
* Corresponding author's Email: Alaa.k.farhan@uotechnology.edu.iq

Abstract: The continuous development in the digital world and the significant increase in the use of digital images have made it important to guarantee protection in the digital world. In the field of security, the advancement of cryptographic algorithms is essential. Recently, cryptography relying on chaotic systems has been suggested as a reliable and effective approach for image protection. Chaos systems have been widely used in security applications due to their good features such as being unpredictable, dynamic, and sensitive to starting conditions and control parameters. The paper presents a new idea for a color image enciphering scheme and creates S-Box based on the 2D-HSM chaotic map. The main contribution of this scheme is how to create and design a new S-Box against many attacks methods. The designed S-Box succeeds all the S-box test standards such as balanced, completeness, avalanch, and strict avalanch. Besides that, enciphering work evaluation parameters such as information entropy, correlations coefficient, histograms, NPCR, and UACI are collected. According to the findings, the entropys, NPCR, and UACI scores obtained for the baboon image are 7.996, 99.64%, and 33.57%.

Keywords: Color image, Chaos, S-Box, RGB, Cryptography, 2D-HSM.

1. Introduction

The growth of communication networks has significantly raised the need for various kinds of encryption algorithms to secure information. The necessity for diverse encryption techniques to secure information transmitted via networks has considerably increased as a result of the development of communication in networks [1]. Multimedia information is considered one of the most vital sources supplied over the internet, it includes photos, videos, and sounds. This information's secure transmission is now the main concern. As a result, digital picture encryption is one of the cryptography study areas that is most active [2]. Grayscale and colour images have recently been the focus of research, with colour images being more appealing since they convey more information than grayscale images [3]. Numerous researchers have been developed numerous methods to secure color images, including hyper chaotic & genetic code [4], alternate quantum walks [5], DNA coding [6], henon system [7], cell neural networks [8], genetic algorithm and matrix semi-tensor products [9], lorenz and ginger breadman chaos theory [10], chaos encryption [11], amplitude-phase encode and discrete complex random transformations [12], combined hashing algorithm and cyclic shifts, and probabilistic symmetric in enciphering relied on chaotic [14]. As new cryptosystems, the data encrypting standard and the advanced encrypting standard are also used to encrypt image [15], but they are not good for images because they have a lot of information and strong connections between pixels.

Chaotic systems are dynamic systems with strong properties like unpredictable, random-like behaviours, system's parameters and conditions sensitive [16, 17]. Henon map and sine map are two systems of chaotic were combined by [18] to produced two-dimensional henon and sine map (2D-HSM), is proposed to overcome the limitation that exist between henon and sine map.

The substitution box (S-Box) is the nonlinear function employed in the block ciphers [19]. To make block cipher algorithms have good security, numerous researchers concentrated on developing strong S-Boxes using chaotic models. In 2012, M. Khan et al [20] developed good SBox by using the Lorenz map. Some of standards which used to analysis results of the suggested S-Boxes such as linear equivalence, bit independence, nonlinearity, stringent avalanche, differential approximation, and in 2016, Maram and Gnanaskar [21] developed a new S-Boxes using a pseudorandom number generators and public key. The analysis results of the suggested S-Box were good and make it suitable to be employed in cryptosystems. In 2017, Dragan Lambc [22] presented a method for designing an S-Box using discrete logistic map. The results of the analysis of the suggested S-Boxes showed the proposed S-Boxes have strong encryption features. In 2019, Q. Lu et al. [23] suggested a novel system to create S-Boxes using hyper-chaos systems (chaotic and ten-logistic maps) (TLS). In the first, a novel linear map was used to construct the original S-Box, which was then scrambled by the TLS. The analysis results of the constructed S-Boxes showed that the generated S-Boxes have more security than other SBoxes. In 2021, G. Hanchinmani [24] presented a novel method of constructing S-box by combining the more than one chaos map. The constructed S-Box met the S-Boxes criteria and was better than other S-Boxes. In 2021, M. Fadhil. [25-27]

in this work the main difference between previous works, many authors depend only on parameters when using chaos theory to present power for this work, but in the proposal designed, we spent not only on the parameters when using a new structure to create S-Box with chaos to avoid many attacks as algebra and non-linear. Can we present in work ref [20-24] it’s clear that.

This paper gives two suggestions. The first suggestion is to design a strong S-Boxes by using a two-dimensional henon and sine map (2D-HSM). Another proposal is to create a novel method of encrypting color images and adapt it to work with their physical characteristics, such as massive data and high pixel connectivity, which includes extracting the three color values of the color image, Red (R), Green (G), and Blue (B), and permuting them by rotating row and column and confusing the R, G, and B utilizing the suggested S-Box. Additionally, the generated S-Box satisfies the SBox tests criterion for balanced, completeness, avalanch, and strict avalanch. In terms of entropy, correlations, and differential attacks, the images ciphered by utilizing the constructed S-Box have good outcomes.

My contributions are listed below:

a- A 2-dimensional chaotic Henon and sine map (2D-HSM) is employed to create a developed S-Box.
b- Proposing a novel approach to encode color image relied on the created S-Box.
c- c- Assessing the created S-Box according to S-Box criteria like balanced, completeness, avalanche, and strict avalanche.
d- Applying entropy, correlation, and differential attack to assess the suggested color image encoding method.

The article's remaining sections are ordered as follows: Section 2 explains the chaos theory and describes the 2-dimensional henon and sine map (2D-HSM). Section 3 explains two suggestions approaches, one to constructing S-Box and one to encrypting color images. Section four discusses the experiment and result, while Section five presents the conclusion.

2. Chaos theory

Chaotic theory is a subfield of mathematics, and it is nonlinear, sensitive to starting conditions and control parameters, and its behaviour could not be forecasted [29, 30]. All those attributes achieve the required properties of confusion and diffusion which is necessary to cipher algorithms. Chaos systems have a high level of sensitiveness to their preliminary parameters, so a small modification in the input produces a considerable modification in the outcome [31]. This makes it impossible to forecast the output values of chaotic systems. For example, if two similar chaotic systems differ only in their preliminary parameters, their results will be considerably various [32]. This important attribute of the chaos system's output is referred to as "sensitivity to original conditions". Because of these attributes, many researchers have become interested in employing chaos systems with ciphering algorithms to increase the level of security [33]. The chaotic system can be utilized for system that need protection, like image encrypting algorithm, block cipher and stream cipher, and others. [35].

2D-HSM chaotic map is a combined of two chaotic systems henon and sine map was proposed in [18], it has good chaotic behaviour. Generally, the 2D-HSM chaotic map can be expressed in Eq. (1).

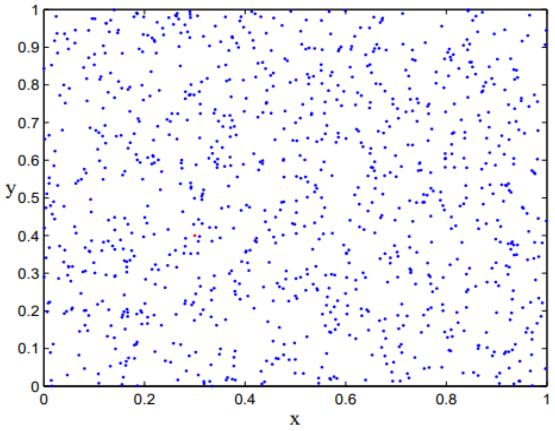

Figure. 1 Trajectories of 2D-HSM

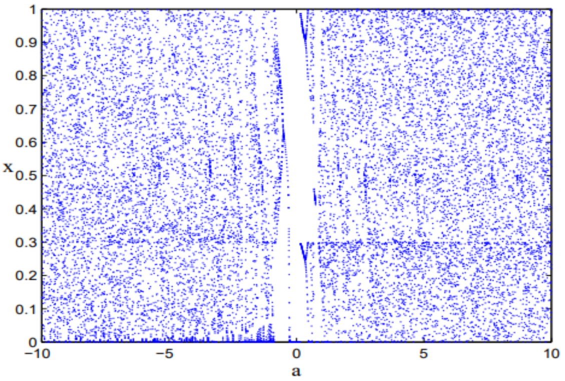

Figure. 2 Bifurcation diagram of 2D-HSM

$$\begin{cases} xi+1 \;=\; (1 \;-\; a * Sin2(x_i) + y_i)\, mod(1) \\ \qquad yi+1 \;=(b * x_i)\, mod(1) \end{cases} \qquad (1)$$

Where (x_0 and y_0) $\in$ (0 to 1) indicate the starting conditions at any time i. (a and b) are a control parameters are expanded to ($-\infty$ to $+\infty$), Fig. 1 explains the trajectories of 2D-HSM. While the bifurcation diagram of 2D-HSM showed in Fig. 2 [18].

3. Research methods

This study presents a developed method for designing S-Box, which is responsible for the confusion process in block cipher, and also presents a developed approach to encrypting color image by utilizing the proposed S-Box with some functions like rotating to obtain the diffusion process. Because chaotic models and cryptography are so complementary, the 2D-HSM chaotic map used to design the S-Box, as explained in Fig. 3. The design of S-Box completed as below: Initially, constructing hexadecimal value using a 2D-HSM chaotic system, and then designing the novel S-Box from the constructed hexadecimal values, for explained in algorithm1. Algorithm2 explains the stages of designing an inverse novel S-Box, I employ it encrypted the color images for my suggested encryption approach.

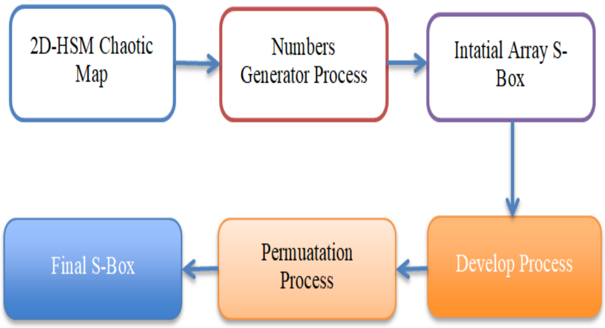

Figure. 3 Constructing of developed S-box

Algorithm 1: Constructing S-Box using 2D-HSM chaotic system

```
Input: starting initial values and control parameters
    ($X_0$, $Y_0$, a, and b) for the 2D-HSM
Output: developed S-Box 16*16
Start:
 1: read $X_0$, $Y_0$, a, and b
 2: generate random sequences of x and y
 3: convert x value into hexa code
 4: convert y value into integer numbers and
      combine it in R // R is a variable
 5: extract two digits from x values (digits 6 and 7)
    and store it in H// H is temporary variable
 6: if H not exist in S THEN // S is string array
    6.1: insert H in S
    6.2: ELSE go to step 2 to generate another value
 7: repeat steps 2,3,4 and 5 until the array has
      completely 256 values
 8: extract 4 digits at one time from R and apply the
      modular by 257
 9: IF The result from step 8 is not exist in P THEN
      // P represent permutation array
    9.1: Insert result of step 8 into P array
    9.2: ELSE go to step 8 to extract another number
 10: repeat steps 8 and 9 until the P array has
      differently order 256 number from 1 to 256
 11: permute the S array by using the permutation
      array (P) resulted by step 10
 12: store the result in S-Box// S-Box represent the
      substation box
End
```

3.1 The suggested construction stages for the S-Box and inverse S-Box

The developed S-Box is constructed as below:

Received: July 14, 2023. Revised: September 9, 2023.

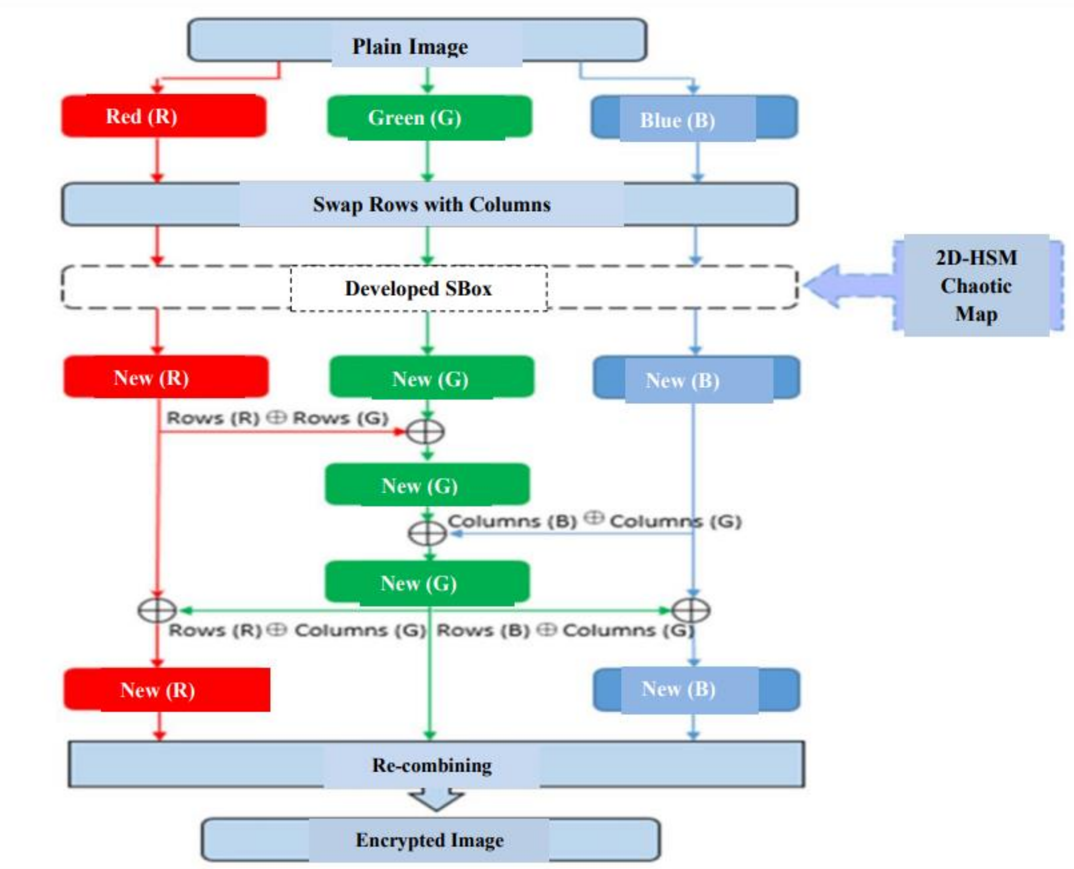

Figure. 4 Color image encryption approach

```
Algorithm 2: Inverse for constructed S-Box
Input: S-Box constructed from algorithm one
Output: invers S-Box  as 16*16
 Start:
   1: Loop all value in S-Box
   2: get the indexes of row and column of one value
      at time from S-Box then combine them together
      and insert it in inverse S-Box// inverse S-Box
      represent the array of inverse substation box
   3: repeat step 2 until generate all value of invers
      S-Box
 End
```

(1) Read the starting conditions and control parameters from the input (2) generating the x and y random sequences and converting the x values to hexadecimal values; converting the y values to integer numbers; extracting two digits from the x hexadecimal values beginning with digit 6 and inserting them in a 16*16 array while ensuring that the values do not repeat. Repeat step2 until getting 256 values. (3) Generate a permutation array by extracting 4 digits from the value of y at a time. (4) Permute all values of the array that was generated in step 2 by using the permutation array that was generated in step 3. The result from step 4 represents the constructed S-Box that can be employed in the block cipher algorithms. Algorithm1 shows the S-Box construction steps.

In order to recover the plain-text during the decryption process, Algorithm two describes how to generate the inverse of the created S-Box.

3.2 Encrypting color image steps

After constructing the developed S-Box, the proposed color images encryption method was employed is encrypted the color images as explain in Fig. 4 and as followed: (1) extracting the basic color of a sensitive images (R, G, and B) channel. (2) Exchange rows with columns of each color (R, G, and B) to achieve to make the diffusion as seen in Fig. 5. (3) Performing the developed S-Boxes on the (R, G, and B) channel to achieve the confusion principle. (4) Executing a bit-wise XOR process function on the values of rows of colors R and G channel to construct mix color of G values. (5) Executing a bit-wise XOR process function on the numbers of columns color B and the new color G to construct new values color G values. (6) executing a bit-wise XOR process function between the values of the row of the color R rows and the values of the columns of the novel color G to obtain a novel color

Table 1. The BC test result of the generated S-Box compared with related S-Boxes

Methods	Words			
	"Computer"		"ABMNOPQR"	
	Zeroes	Ones	Zeroes	Ones
[20]	38	26	31	33
[21]	35	32	31	32
[22]	32	32	34	28
[23]	33	31	29	35
[24]	29	35	32	28
[25]	32	32	33	31
Suggested S-Box	**32**	**32**	**32**	**32**

R values and, concurrently, executing a bit-wise XOR process function between the values of the rows of the color B and the values of the columns of the novel color G to getting a novel color B. (7) combining the values of colors that were resulted from step 6 to construct the completed ciphered image. The method of decrypting is the opposite of the processes that came before, and it uses the opposite of the S-Box.

4. Results and discussion

The S-Box and its inverse are constructed in only 4 milliseconds. In addition, the created S-Box satisfied the S-Box criterion for balance, completeness, avalanches, and strict avalanches. Furthermore, the images that were ciphered by utilizing the created S-Box obtained excellent outcomes in regards of entropy, correlations, histograms, and differential attacks. All of the S-Box criterion and image encryption measures are explained in detail below. All of the outcomes were compared to similar studies.

4.1 S-Box criteria

Some of test in S-Box can see in:

4.1.1. Balanced criterion (BC)

One of the most essential S-Box criteria is to test the frequency of the zeros and ones in the output sequences, which must be balanced [36, 37]. This test utilized two strings with the generated S-Box and the outcomes shows that the generated S-Box is balanced due it has an equal amount of zeroes and ones, as seen in Table 1.

Figs. 5 and 6 display the BC results of the generated S-Box and the S-Boxes of the related studies. Whereas Fig. 5 displays the amount of zeroes and ones after replacing the word (Computer) with new text from generated S-Box, Fig. 6 displays the amount of zeroes and ones after replacing the word "ABMNOPQR" with new text also from generated S-Box. It is noting that the generated S-Box has more balanced 0's and 1's than other S-Boxes. This indicates that the S-Box generated satisfies the BC requirement.

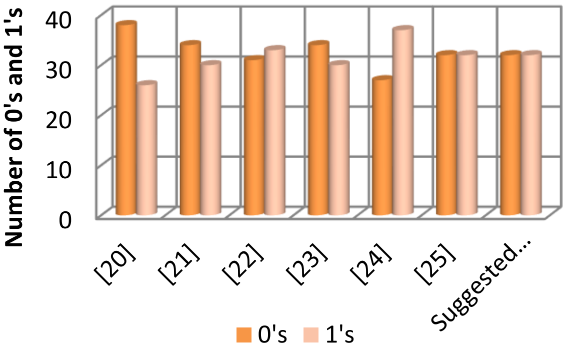

Figure. 5 Comparison of the BC test results of the constructed S-Box and other related S-Boxes for the word "Computer"

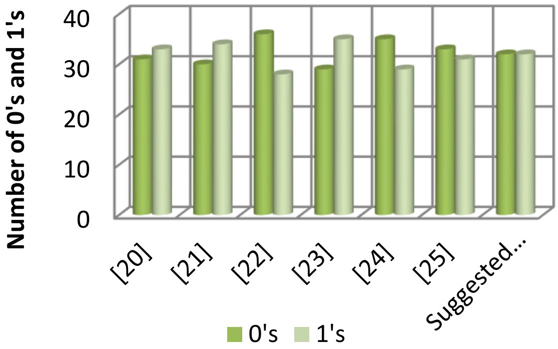

Figure. 6 Comparison of the BC test results of the constructed S-Box and other related S-Boxes for the word "ABMNOPQR"

4.1.2. Completeness criteria (CC)

This test defines as completenes, that means each output bit is based on the full input bits effective [38]. Tables as 2, 3, 4, and 5 shows that the constructed new S-Boxes passes from this test because each bit of the output is dependent on the entire input bits (starting conditions and parameters (x, y, a, and b).

4.1.3. Avalanche criterion (AC)

In the block ciphers, the lack of any relation between input bits and output is very important, indicating that the system has good features, which is defined by utilizing the AC test to indicate that a small modification in plain-text results in a

Table 2. S-Box constructed from the inputs x_0=0.0131, y_0,=0.5 a=1.28 and b=0.3

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

Table 3 Invers S-Box from inputs x_0=0.0131, y_0,=0.5 a=1.28 and b=0.3

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

Table 4. S-Box constructed from the inputs x_0=0.0231, y_0,=0.4 a=1.27 and b= 0.3

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

Table 5. Invers S-Box from inputs x_0= 0.0231, y0,=0.4 a=1.27 and b= 0.3

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

Table 6. Comparison of the AC test results of the constructed S-Box and other related S-Boxes

S-Boxes	**Original later**	**Binary in**	**Binary out**	**AC**
[20] modifying single bit	L M	01001100 01011101	10110100 00100111	4/8 = 0.50
[21] modifying single bit	L M	01001101 01011101	11111011 01100001	4/6= 0.66
[22] modifying single bit	L M	01011100 01011101	01111100 01111100	5/6= 0.62
[23] modifying single bit	L M	01011100 01001101	10111110 01100111	4/8 = 0.5
[24] modifying single bit	L M	01011100 01011101	10110001 01000101	3/7 = 0.42
[25] modifying single bit	L M	01000011 01101100	10010101 10110000	5/8 = 0.62
Suggested a S-Box modifying single bit	L M	01001100 01001101	01001101 01100000	4/8 = 0.5

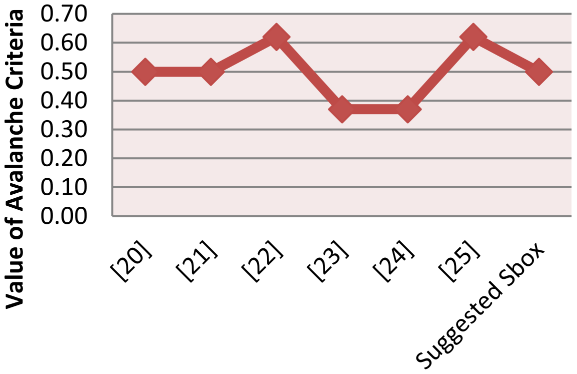

Figure. 7 AC test for the generated S-Box and comparison with another S-Boxes

Table 7. entropy outcomes with comparison to the similar studies

methods	**images**	**Entropy (Average)**
Suggested method	Lena	7.998
	Baboon	7.996
	Woman	7.994
	Peppers	7.996
[9]	Lena	7.997
[10]	Peppers	7.995
[11]	Lena	7.994

significant modification in cipher-text, like modifying one bit from zero to one, or inversely, resulting in a significant modification in output. The score of this test is determined utilizing Eq. (2) and is measured between 0 and 1, where the best value is 1/2, which means it passes the avalanches criterion [38]. Table 6 displays the AC test.

$$AC = \frac{No.\ Modified\ Bits\ in\ CipherText}{No.\ All\ Bits\ in\ CipherText} \qquad (2)$$

Table 8. Outcomes of correlation coefficient

Images name	**Correlations (Averages)**
Lena pic	0.00264
Baboon pic	0.00241
Woman pic	0.00211
Peppers pic	0.00201

To test the suggested S-Box, I modified one bit of the string "L" to be "M" and changed each of "L" and "M" with new value from the suggested S-Box. The outcome of "L" differed from "M" in four of the total eight bits. According to Eq. (2), the AC value obtained is 0.5, which indicates that the constructed S-Box meets the avalanched criteria. The outcomes of this test are also compared to the outcomes of other similar work, as seen in Table 6 and Fig. 7.

4.1.4. Strict avalanche criteria (SAC)

The S-Box satisfies the SAC when changing a single input bit results in a modify in half of the output bits [39, 40]. The SAC test is true when both the AC and CC tests are passed [41, 42]. So, since the suggestion passes the AC and CC tests, it also passes the SAC test.

4.2 Metrics for encrypted images

4.2.1. Information entropy

Entropy is a metric of the random information in an image. The high entropy in an image indicates that the image has more random information [43, 44]. Eq. (3) is employed to define the entropy. The entropy must be near to or equals to 8 [45].

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

Where $P(H_i)$ is the probability of pixel H_i in an image.

According to Table 7, it is seen that the entropy result of the suggested approach is very near to eight, meaning it is difficult to predict the pixel values in the image. As compared to related studies, the suggested approach is the best.

4.2.2. Correlation coefficients

This is a statistical evaluation utilized to define the relationship between the pixels of the initial image and the ciphered image. To fulfil this test, the correlation coefficient should be close to zero. [46]. Eq. (4) is employed to define the correlation coefficient.

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

Table 9. Comparison of NPCR and UACI results

methods	**images**	**Averages NPCR$_{R,G,B}$ (%)**	**Averages UACI$_{R,G,B}$ (%)**
Suggested method	Lena	99.61	33.69
	Baboon	99.64	33.57
	Woman	99.57	33.64
	Peppers	99.64	33.58
[12]	Lena	99.58	33.66
[13]	Lena	99.59	33.55
[14]	Lena	99.58	33.50

As noted in Table 8, the correlation coefficient for each used image is near to 0, which means there is very little correlations existing among pixels in all ciphered images.

4.2.3. Histogram analysis

A histogram displays the frequency of occurrence of pixel values in original and ciphered images. the histogram distribution of the ciphered image should be uniform and flat to remove the image's statistical attribute , which are used by the attacker [9, 45, 47]. The histograms of the 4 original and ciphered images are seen in Fig. 8. The comparison shows that the encrypted image histograms are nearly flat. As a result, statistical assaults do not provide the attacker with any meaningful information.

4.2.4. Differential attack

The proposed images ciphering scheme has been evaluated for differential attacks on 4 images by using the number of pixels changing rate as (NPCR) with unified averages changing intensity as (UACI) which are defined for a L.H images size employing Eq. (5) [48] and (6) [46].

$$NPCR = \left[\frac{\sum_{i,j} I(i,j)}{L.H}\right].100\ \% \quad (5)$$

$$UACI = \frac{1}{L.H}\left[\frac{\sum_{i,j}\left|C^1(i,j) - C^2(i,j)\right|}{255}\right].100\ \% \quad (6)$$

Where I(i, j) = 1 ifC1(i, j) ≠C2 (i, j), otherwise I (i, j) =0 and C1 and C2 show the ciphered images of original image before and after single-pixel modification in the original image [49], [50]. For testing, a single pixel of the original image is modified to get the ciphered image C2. The results of the NPCRs with the UACIs for the four images are shown in Table 9 with comparison to similar studies.

According to Table 9, the suggested approach is sensitive to single pixel alterations and outperforms the [12, 13, and 14] methods.

4 Conclusion

The present research suggests a diffusion and permutation-based color image encryption method

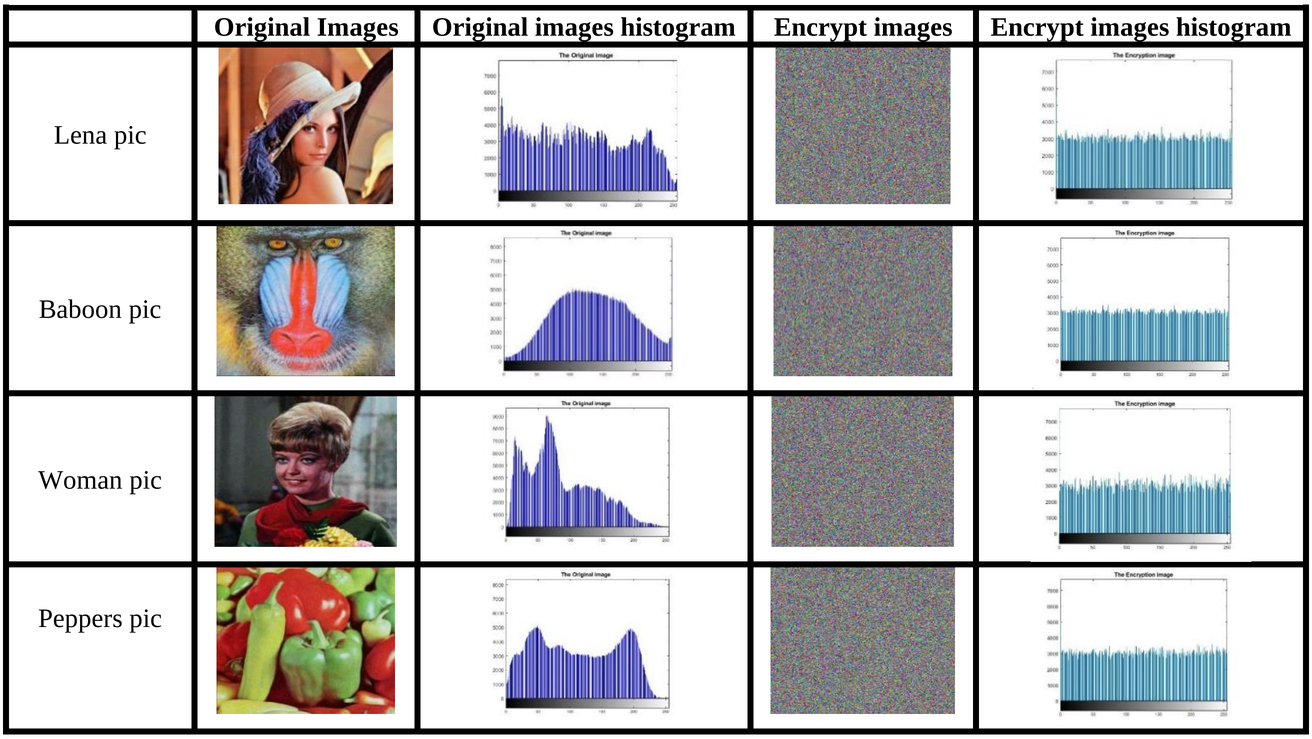

Figure. 8 Histogram analysis

based on a newly built S-Box made with a 2D-HSM chaotic map. The newly built S-Box met the stringent, balanced, complete, and avalanched criterion for the testing S-Box. This shows that the recommended S-Box has favorable cryptographic attributes. It was developed in just 4 milliseconds and could be used with other lightweight systems as well as the advanced encrypting standard (Block Cipher). The suggested color picture encryption approach additionally improves histogram uniformity, correlation coefficient, and entropy amount, UACI and NPCR. Information entropy, NPCR, and UACI findings for the Baboon image are 7.996, 99.64%, and 33.57%, respectively. These results are more advanced than those of the analogous studies. These findings demonstrate that the information entropy is quite close to eight. This demonstrates the high security of the suggested color image encryption method. Future research could make use of higher-dimensional chaos to create.

Conflicts of interest

No conflict of interest has been announced by all authors.

Author contributions

The idea for the article was the first author's, the software and methodology were the second author's, and the actual analysis, data curation, validation, resource management, writing a review, editing, writing original draft preparation, and visualization were the third author's to handle. The previous author was in charge of project management and oversight.

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. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in colour images", *Signal Processing*, Vol. 164, pp. 163–185, 2019, doi: 10.1016/j.sigpro.2019.06.010.

[4] H. Nazir, I. Bajwa, S. Abdullah, R. Kazmi, and M. Samiullah, "A Colour 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, "Colour Image Encryption Scheme Based On Alternate Quantum Walk and Controlled Rubik's Cube", *Sci. Rep.*, Vol. 12,

pp. 0–14, 2022, doi: 10.21203/rs.3.rs-1204955/v1.

[6] I. Aljazaery, H. ALRikabi, and A. Alaidi, “Encryption of Colour 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] A. Alhudhaif, M. Ahmad, A. Alkhayyat, N. Tsafack, 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.

[8] R. Zhang, L. Yu, D. Jiang, W. Ding, J. Song, K. He, and Q. Ding, “A novel plaintext-related colour 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 colour image encryption”, *Signal Processing*, Vol. 183, p. 108041, 2021, doi: 10.1016/j.sigpro.2021.108041.

[10] F. Khan, J. Ahmed, J. 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. 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] A. Kadhim and R. M. Mohamed, "Visual cryptography for image depend on RSA & AlGamal algorithms", In: *Proc. of 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, 2016, pp. 1-6, doi: 10.1109/AIC-MITCSA.2016.7759935.

[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 Colour Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method Improved Colour 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.

[16] C. Pak and L. Huang, “A new colour 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] J. Wu, X. Liao, and B. Yang, “Image encryption using 2D Hénon-Sine map and DNA approach,” *Signal Processing*, Vol. 153, pp. 11–23, 2018, doi: 10.1016/j.sigpro.2018.06.008.

[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] S. Marochok and P. Zajac, "Algorithm for Generating S-Boxes with Prescribed Differential Properties", *Algorithms*, Vol. 16, No. 3, p. 157, 2023, doi: 10.3390/a16030157.

[22] W. Yan and Q. Ding, "A Novel S-Box Dynamic Design Based on Nonlinear-Transform of 1D Chaotic Maps", *Electronics*, Vol. 10, No. 11, p. 1313 2021, doi: 10.3390/electronics10111313.

[23] H. Alsaif, R. Guesmi, A. Kalghoum, B. M. Alshammari, and T. Guesmi, "A Novel Strong S-Box Design Using Quantum Crossover and Chaotic Boolean Functions for Symmetric Cryptosystems", *Symmetry*, Vol. 15, No. 4, p. 833, 2023, doi: 10.3390/sym15040833.

[24] F. Sbiaa, M. Machhout, and M. Zeghid, "Design and SystemC Implementation of Chaos-Based Enhancements for the Advanced

Encryption Standard", In: *Proc. of 2017 27th International Conference on Computer Theory and Applications (ICCTA)*, Alexandria, Egypt, pp. 50-56, 2017, doi: 10.1109/ICCTA43079.2017.9497217.

[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*, 2021, Vol. 1076, No. Isces 2020, pp. 1–12, 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. E. 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] H. Liu and X. Wang, "Cryptanalyze and design strong S-Box using 2D chaotic map and apply to irreversible key expansion", *arXiv preprint arXiv:2111.05015*, 2021, doi: 10.48550/arXiv.2111.05015.

[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, 2014, pp. 231–236, 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, "Colour 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. A. Khaldi, 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 colour 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 colour 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.