Basrah Journal for Engineering Sciences, Vol. 24, No. 2, (2024), 68-73

Original Article

Journal homepage: www.bjes.edu.iq
ISSN (Online): 23118385, ISSN (Print): 18146120

S-Box Design Utilizing 3D Chaotic Maps for Cryptographic Application

Jenan Ayad Namuq [1, *]

[1] *Department of Electro-Mechanical Engineering, University of Technology, Baghdad, Iraq*
E-mail addresses: jinan.a.namuq@uotechnology.edu.iq
Received: 30 June 2024; Revised: 26 July 2024; Accepted: 1 August 2024; Published: 17 August 2024

Abstract

In the realm of cryptography, the Substitution-box (S-box) is a critical component for enhancing the security of encryption algorithms. The inherent characteristics of Chaos, such as sensitivity to beginning conditions and unpredictability, make it a highly suitable choice for encryption applications. In this paper, proposed a method for generating S-Boxes using 3D chaotic maps algorithms including (Cat map, Henon map, Sine map, and Cosine map). The primary focus is on enhancing the security and efficiency of cryptographic systems by leveraging the inherent complexity and unpredictability of chaotic maps. The design methodology focuses on achieving high non-linearity, optimal avalanche effect, and Strict Avalanche Criterion (*SAC*), ensuring that minor changes in plaintext result in significant alterations in the ciphertext. Our study presents a detailed analysis of the generated S-Boxes, demonstrating their robustness against common cryptographic attacks. Key findings include significant improvements in nonlinearity, differential uniformity, and bijectivity compared to traditional methods. The test findings and performance analysis indicate that our proposed S-Box exhibits much lower values of Linear Probability (*LP*) and Differential Probability (*DP*), while maintaining a suitable average value of nonlinearity. Additionally, discussed the broader implications of our findings, emphasizing how the proposed method can be employed to produce high-quality analytical results that enhance the security measures of cryptographic applications. This work adds valuable context to existing research and highlights the potential for our model to outperform conventional S-Box generation techniques.

Keywords: S-Box, 3D chaotic map, Encryption, Decryption, Cat map, Henon map.

https://doi.org/10.33971/bjes.24.2.9

1. Introduction

Over the past few years, there has been substantial advancement in the field of image processing technologies and communication networks. Ensuring the protection of sensitive information throughout both wired and wireless communications is crucial because of the immediate movement of data [1-3]. The utilization of multimedia and visual content has become widespread in various domains, encompassing the transmission of military and medical personnel data. In the past, conventional encryption methods were employed to encrypt photos, but their effectiveness was inadequate for encrypting larger images [4-6]. For this reason, research has been conducted into the development of several image encryption techniques. Chaos-based encryption research is one of these subjects [7-10]. There is a strong correlation between chaotic systems and cryptology [11]. Chaotic systems possess randomness, beginning parameters, control sensitivity, and ergodicity, which fulfill the fundamental criteria of cryptology [12, 13]. The deterministic and extremely unpredictable nature of values created by chaotic systems provides a substantial benefit for encryption systems. These qualities have been utilized to conduct more research on encryption based on chaos [14-17]. Random number sequences are produced by random number generators specifically for the purpose of encryption [18-20]. The S-Box is a crucial component in block encryption systems, responsible for executing confusion operations. Utilizing a robust S-Box structure enhances the security of encryption. S-Box structures must have high cryptographic features, be resistant to attacks, and resist differential cryptanalysis in order to be used for encryption [21-23]. Substitution-Box basically consists of a number of mathematical operations. It takes as an input a block of plaintext and a key and applies S-box to get the desired cypher text. For the decryption process, the inverse S-box is used in reverse order with the same key [24].

1.1. Related works

The complex structures of modern encryption algorithms, which require a great deal of computing power, have a negative impact on the efficiency of encryption operations. Encryption studies based on chaotic systems and substitution box are incredibly prevalent in the academic literature, but it can be observed that studies employing only one type of encryption technique contain certain flaws [25].

Setyaningsih et al. [26], before encryption, the encrypted data, which consists of S-Boxes generated based on a chaotic logistic map, was compressed. Alanazi [27], proposed a 3D chaotic map and highly nonlinear S-boxes for the encryption before transitioning to a data concealment scheme based on the Lah transformation. Jun and Fun [28], they employed a low-dimensional chaotic scheme in order to create an S-box with dimensions of 10 by 26. Tanveer et al. [29], they increased the efficacy of encryption and promoted secure transmission according to the presented 3D chaotic map-based symmetric

approach for multiple images. Abduljabbar et al. [30], hypothesized that by combining numerous chaotic map types with an S-box, a fast method for scrambling and encrypting color images might be achieved. Deb and Behera [31], they utilized Henon map to propose new image cryptosystem key-dependent bijective S-Boxes.

This work focuses on utilizing simple procedures to construct a robust and secure S-Box algorithm. The remaining parts of this work are structured as described below. Section 2 contains the 3D chaotic maps used with the proposed S-Box. In Section 3, S-box construction and the properties of these signals. The results of the experiments and an appraisal of their effectiveness are presented in Section 4. In the end, the conclusions are discussed in the final section.

2. Methodology

This method is providing a secure and strong key construction in a non-linear way that can confront attacks and also it is can be used to enhance the encryption system by cascading this algorithm with other techniques.

2.1. Chaotic maps

Many different chaotic systems have been used in the literature. The most famous 3D chaotic systems (Henon map 30, Sine map 29, Sine-Cosine 32, and Cat map 33) have been considered for testing the proposed systems. The mathematical models of the chaotic systems used in this study are defined in Table 1.

Table 1. Chaotic maps.

Chaotic map	Mathematical model	Initial values	Control parameters
3D Sine-Cosine 3D CSM [29]	$x_{n+1} = W^m \sin(x_n) + y_n - H^m \cos(z_n)$ $y_{n+1} = \sin(x_n)\cos(y_n) + x_n + \tan(z_n)$ $z_{n+1} = y_n\ cos\ (x_n)\ + B^m x_n \sin(z_n)$	$x_0 = -0.0005$ $y_0 = 0.300001$ $z_0 = -0.38$	W = 0.66 H = 1.33332 B = 15.13 m = 5
3D Henon map 3D-HM [30]	$x_{n+1} = a - {y_n}^2 - bz_n$ $y_{n+1} = x_n$ $z_{n+1} = y_n$	$x_0 = 0.17$ $y_0 = 0.45456$ $z_0 = 0.9434$	a = 1.76 b = 0.1
3D Sine map 3D-SCM [32]	$x_{n+1} = \sin\left(a_1 \sin^{-1}\sqrt{x(i-1)}\right)^2$ $y_{n+1} = \sin\left(a_1 \sin^{-1}\sqrt{y(i-1)}\right)^2$ $z_{n+1} = \sin\left(a_1 \sin^{-1}\sqrt{z(i-1)}\right)^2$	$x_0 = \sin(\theta_1 \pi a_1)^2$ $y_0 = \sin(\theta_2 \pi a_2)^2$ $z_0 = \sin(\theta_3 \pi a_3)^2$	$\theta_1 = 60, a_1 = 4$ $\theta_2 = 70, a_2 = 3$ $\theta_3 = 80, a_3 = a_1 \times a_2$
3D Cat map 3D CM [33]	$x_{n+1} = (3x_n + y_n + 4z_n) mod\ 1$ $y_{n+1} = (6x_n + 3y_n + 11z_n) mod\ 1$ $z_{n+1} = (6x_n + 2y_n + 9z_n) mod\ 1$	$x_0 = 0.7467$ $y_0 = 0.3394$ $z_0 = 0.65758$	

2.2 The S-Box construction

The substitution function sb (s, p) is defined to describe the nonlinear transformation of the pixel value p using the S-box matrix s. The S-box transformation is implemented utilizing a three-dimensional chaotic map. The function value is the transformed ciphertext pixel value. Based on the chaotic maps (3D-CM, 3D-HM, 3D-SCM), an algorithm for the construction of dependable S-boxes has been proposed. The generated 3D chaotic sequences are arranged in ascending order, and the corresponding indices of the sorted data are saved in an array. The array stores the values that have been sorted. The sorting process is of utmost importance in order to generate the subsequent S-box. The indices that have been sorted are transformed into a matrix of dimensions 16 × 16, which is referred to as (Sbox_matrix). The matrix provided above serves as a representation of the S-box, wherein each element corresponds to the index of the sorted sequence values that have been formed. The S-box transformation is applied to every pixel in the supplied image. The pixel's value serves as an index for retrieving the appropriate value from the S-box. The value obtained from the retrieval process is subsequently saved as the updated pixel value within the modified picture, denoted as (Sbox_Imag), which is the ciphertext pixel value obtained.

The construction of an S-box begins with the execution of the three phases listed below:

Step 1: Construct a chaotic sequence based on one of the chaotic maps or the proposed methods.
Step 2: Sort the sequence randomly by its index.
Step 3: Use the index as decimal values map to obtain the final S-box sized of 16 × 16.

Algorithm 1 illustrates the precise procedure for constructing an S-box and chaotic sequences.

Algorithm 1 S-Box with chaotic map

Input: An image of size $m \times n$ and a chaotic sequence (x_i, y_i, z_i).
Output: The substituted image Sbox_Imag.
1. Sort the chaotic sequence x by its indices to get [xs].
2. Generate a 16 × 16 substitution matrix Sbox_matrix using the index vector from the sorted sequence.
3. For each column $k1$ from 1 to n.
4. For each row $k2$ from 1 to m.
5. Substitute the pixel value in the image by the corresponding index in the substitution matrix and store it in Sbox_Imag.

The construction of a new S-box, denoted as S, should have the following conditions:

- The size of S is 16 × 16; this can hold a maximum of 256 individual items.
- Each element of S must be a positive integer from 0 to 255 for S to be valid, such that S $(i, j) \in [0, 255]$.
- No two entries in S (i, j) must be identical, and the range 0-255 must be covered by 256 different values, such that $S(i, j) \in [0, 255]$.

To decrypt, we must define an S-box inverse transform function, sb Inverse (s, q). The second algorithm outlines the stages involved in S-box inverse substitution.

Algorithm 2 Inverse S-Box with Chaotic Map

Input: Substituted image Sbox_Imag of size $m \times n$ and a 16 × 16 S-Box matrix.
Output: $m \times n$ image InvSBox_Imag.

1. For each i from 1 to 256.
- For each j from 1 to 256.
- If the index x equals i.
- Assign the value of j to the index y.
2. For each column $k1$ from 1 to n.
- For each row $k2$ from 1 to m.
- Retrieve the image pixel value from the index and subtract 1, storing it in InvSBox_Imag.

3. Results and discussion

In this study, S-Box was generated by the Henon map, Cat map, and Sine map. Table 2 illustrates example of the constructed S-box for Henon chaotic map. The algorithm was executed by MatLab program 2021 b.

The significance of the S-box in attaining confusion and non-linearity during the encryption procedure becomes apparent when examining the statistical analysis of the cipher's efficacy [34-37].

The S-box, which has been meticulously crafted, has strong resilience against a range of cryptanalysis methods, including differential and linear attacks, which confirms its effectiveness in 113 preventing potential security vulnerabilities.

The results of the experiment highlight the crucial role played by the S-box in strengthening the encryption scheme as a whole, which confirms its significance in protecting sensitive data from unauthorized access and ensuring the system's ability to withstand contemporary cyber threats. The results of cryptographic properties of the S-box are evaluated by some parameters like balanced, bijective, non-linearity, avalanche value, and absolute indicator).

During our cryptographic evaluation of the suggested S-box, the traditional S-box performance evaluation criteria were utilized. The performance of the proposed S-box in terms of cryptography is summarized in Table 3, and the results of a comparison of the previous S-boxes are shown in Tables 4 and 5. A Boolean function S: GF(2n) → GF(2) is called balanced if the output set contains an equal number of ones and zeros in the corresponding truth table. A Boolean function S: GF(2n) → GF(2) is bijective if and only if all linear combinations of columns are balanced. A point is called a fixed point of the S-box if S(u) = u, and a point is called the opposite fixed point of the S-box if S(u) = u`. Strong S-boxes have high Nonlinearity values and can perform nonlinear input-to-output transformations. These S-boxes facilitate the prevention of linear cryptanalytic attacks against plaintext data.

It can be seen from this table that all the vectors are balanced and the output distribution is evenly distributed across the output space, resulting in a balanced distribution and bijective (possessing both injective and surjective properties). The concept of non-linearity measures the extent to which a function diverges from linearity, where the maximum non-linearity is 120, and subsequently the vectors have a high non-linearity. The Self-Avalanche 118 Criterion (SAC) quantifies the extent to which changes in the input of a system propagate to the output, hence evaluating the phenomenon known as the (avalanche effect). A value of 0.5 indicates that the alteration of a single input bit leads to an approximate 50% change in the output bits. Based on the data presented in the table, it is evident that the SAC values for all vectors exhibit a uniform value of 0.5, which is considered to be the optimal value.

Table 2. presents an S-box that has been created using the Henon chaotic map.

i/j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	57	79	88	52	202	222	207	66	176	33	118	54	4	14	163	19
2	71	158	140	32	227	185	121	24	115	180	219	120	150	125	130	95
3	29	82	212	167	43	173	55	7	188	168	114	17	189	246	98	160
4	12	206	108	91	255	106	69	100	149	92	191	228	116	236	22	84
5	123	68	175	74	3	210	27	132	200	75	49	128	177	241	64	136
6	234	26	187	60	45	138	10	153	225	61	196	221	110	251	154	208
7	37	9	148	143	58	86	232	63	41	144	145	249	214	39	133	104
8	184	231	199	194	72	162	35	146	253	195	62	239	46	223	101	171
9	172	102	224	47	30	129	182	197	243	48	152	244	193	198	230	183
10	105	134	40	215	13	97	170	50	238	113	6	44	142	147	8	36
11	209	155	252	111	124	21	103	165	248	218	203	256	59	186	25	233
12	137	65	242	178	245	229	135	89	220	216	76	2	73	174	67	122
13	85	23	237	117	235	80	94	141	127	217	93	254	90	107	205	11
14	161	99	247	190	240	18	77	192	16	1	169	42	166	211	81	28
15	96	131	126	151	250	159	156	213	119	112	181	226	31	139	157	70
16	20	164	15	5	38	83	204	109	53	179	34	201	51	87	78	56

Table 3. S-Box performance evaluation.

S-Box test	Henon	Cat	Sine
Balanced	Yes	Yes	Yes
Bijective	Yes	Yes	Yes
Non L. S	104	102	102
Non L. B.F	94	104.25	102
SAC	0.5	0.5	0.5
BIC-NL	100	103.78	104
BIC-SAC	0.4063	0.4063	0.4375
DP	0.1328	0.1328	0.1328
LP	0.125	0.125	0.125
AC	0.5	0.5	0.5
Fixed & Opp.	2,0	1,0	0,1
HW	128	128	128

The BICNL (Bit Independence Criterion - Nonlinearity) metric assesses the degree of independence between output bits and input bits, while simultaneously ensuring favorable levels of non-linearity. The majority of the vectors possess values exceeding 100, with the final vector being in close proximity to 100. The BIC-SAC (Bit Independence Criterion - Strict Avalanche Criterion) amalgamates the fundamental principles of BIC and SAC. The measurement assesses the level of bit independence, taking into account the rigorous avalanche requirement. The vectors exhibit values that are approximately 0.5. The criterion Avalanche Criterion (AC) is used to evaluate how changes in the input of a cryptographic function propagate to the output, ideally leading to significant changes in the output even for minor changes in the input. This property is crucial for ensuring that the cryptographic function resists differential cryptanalysis. The concept of Differential Probability (DP) pertains to quantifying the probability of a particular disparity in input bits resulting in a corresponding disparity in output bits. Lower values are indicative of greater resilience to differential attacks. The numbers depicted in the table have an approximate magnitude 0.13. The concept of Linear Probability (LP) refers to the likelihood that a given

linear approximation accurately represents the relationship between input and output bits within a function. All vectors have the same value of 0.125, where the smaller the value of LP the better the performance. Fixed and opposite test indicates the number of points. The evaluation of an S-box's vulnerability to differential and linear attacks is conducted through the use of fixed and opposite test. This is due to the fact that fixed points and opposite pairs can be effectively exploited in both attack methodologies.

An ideal cryptographic S-box should possess a minimal 119 number of fixed points and should have a balanced distribution of opposite pairings. In this table, the pair 1,2 is the max. pair. The term (HW) is an abbreviation for Hamming Weight, which is a metric used to determine the count of non-zero elements in the binary representation of a given value. This table shows information regarding the distribution of non-zero bits in the output.

According to comparing the proposed S-box with the studies mentioned in Tables 4 and 5, the generated S-box is robust and secure.

4. Conclusions

A method for constructing S-boxes, which are both simple and secure, has been described. This method is based on utilizing 3D chaotic maps to encrypt data. Aiming to reduce the complexity and increase the efficiency of the encryption system, this system has been proposed to encrypt data. Furthermore, by using an S-box. It is feasible for both pixel and key information to be distributed throughout the entire cipher data. A robust substitution mechanism was developed that significantly improves resistance to linear and differential cryptanalysis. Our experimental results demonstrated that the proposed S-Box algorithm achieves high non-linearity, optimal avalanche effect, and compliance with the strict avalanche criterion (SAC). The performance evaluation indicates that our approach not only strengthens cryptographic security but also maintains computational efficiency, making it suitable for real-time applications. Additionally, we proposed an inverse S-Box algorithm that effectively reconstructs the original image from its substituted counterpart, ensuring the integrity and recoverability of the encrypted data.

Table 4. Comparison of S-Box performance with previous studies.

	Balanced	Bijective	Non-Lin	SAC	BIC-NL	BIC-SAC	DP	LP	AC%
[1]	-	-	106	0.42	100	0.47	-	-	-
[2]	-	-	98	0.5	104	0.504	0.047	0.133	-
[7]	-	-	106.3	-	103.9	0.507	0.039	0.133	0.625
[19]	-	-	106	0.4	-	0.48	0.039	0.125	-
[36]	-	-	106.5	0.495	103.8	0.498	0.039	0.141	-
[37]	-	-	104	0.507	103.9	0.507	0.054	0.14	-
[38]	-	-	104	0.4	96	0.48	0.038	0.1328	-
[39]	-	-	98	0.391	103.8	0.462	0.046	0.125	-
[40]	Yes	Yes	96	0.42	96	0.47	0.0469	0.0625	-
[41]	-	Yes	104	0.42	96	0.47	0.039	0.132	-
[42]	-	-	103	0.503	100	0.501	0.5	0.148	-
[43]	-	-	104.7	0.504	104	0.505	0.039	0.1406	-
[44]	-	-	104	0.5026	103.2	0.5033	-	0.1328	-
[45]	Yes	Yes	112	0.453	98	-	-	-	59.37
[46]	-	Yes	106.3	0.42	98	0.47	0.039	0.125	49-50
[47]	-	-	104.5	0.498	104.6	0.508	0.047	0.125	-
[48]	-	-	104	0.4018	103.857	0.4988	-	-	-
[49]	Yes	-	-	0.41	-	-	-	0.33	-

The integration of chaotic sequences in both forward and inverse transformations highlight the versatility and robustness of our method. Overall, the developed S-Box encryption algorithm presents a significant advancement in the field of cryptography, offering a powerful tool for secure communication and data protection. Future work may explore the application of this algorithm in various cryptographic protocols and its potential enhancements through the incorporation of other chaotic systems and optimization techniques.

References

[1] Z. Chen, and G. Ye, "An asymmetric image encryption scheme based on hash SHA-3, RSA, and Compressive Sensing," Optik, Vol. 267, 2022. https://doi.org/10.1016/j.ijleo.2022.169676

[2] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A new image encryption algorithm for Grey and color medical images," IEEE Access, Vol. 9, pp. 37855-37865, 2021. https://doi.org/10.1109/access.2021.3063237

[3] H. I. Mhaibes, M. H. Abood, and A. Farhan, "Simple lightweight cryptographic algorithm to secure imbedded IOT devices," International Journal of Interactive Mobile Technologies (iJIM), Vol. 16, Issue 20, pp. 98-113, 2022. https://doi.org/10.3991/ijim.v16i20.34505

[4] R. S. Ali, O. Z. Akif, S. A. Jassim, A. K. Farhan, E.-S. M. El-Kenawy, A. Ibrahim, M. E. Ghoneim, A. A. Abdelhamid, "Enhancement of the cast block algorithm based on novel S-box for image encryption," Sensors, Vol. 22, Issue 21, 2022. https://doi.org/10.3390/s22218527

[5] J. Ayad, F. S. Hasan and A. H. Ali, "Image encryption using One Dimensional Chaotic Map and transmission Through OFDM system", 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, pp. 1-7, 2023. https://doi.org/10.1109/ICCCNT56998.2023.10308260

[6] J. Ayad, F. S. Hasan and A. H. Ali, "OFDM Transmission for encrypted Images based on 3D Chaotic Map and S-Box through Fading Channel", International Conference on Smart Systems for applications in Electrical Sciences (ICSSES), Tumakuru, India, pp. 1-6, 2023. https://doi.org/10.1109/ICSSES58299.2023.10199452

[7] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," Information Sciences, Vol. 480, pp. 403-419, 2019. https://doi.org/10.1016/j.ins.2018.12.048

[8] J. Ayad, F. S. Hasan and A. H. Ali, "Efficient Transmission of Secure Images with OFDM using Chaotic Encryption", 4th International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, pp. 391-396, 2022. https://doi.org/10.1109/I4C57141.2022.10057774

[9] R. B. Naik, and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," Annals of Data Science, Vol. 11, pp. 25-50, 2022. https://doi.org/10.1007/s40745-021-00364-7

[10] C. Zhu, Z. Gan, Y. Lu, and X. Chai, "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," Multimedia Tools and Applications, Vol. 79, pp. 7227-7258, 2020. https://doi.org/10.1007/s11042-019-08226-4

[11] D. S. Laiphrakpam, R. Thingbaijam, K. M. Singh and M. Al Awida, "Encrypting multiple images with an enhanced chaotic map," IEEE Access, Vol. 10, pp. 87844-87859, 2022. https://doi.org/10.1109/access.2022.3199738

[12] B. Ge, X. Chen, G. Chen and Z. Shen, "Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation," IEEE Access, Vol. 9, pp. 137635-137654, 2021. https://doi.org/10.1109/access.2021.3118377

[13] A. S. Saljoughi, and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," Pattern Analysis and Applications, Vol. 22, Issue 1, pp. 243-257, 2018. https://doi.org/10.1007/s10044-018-0765-5

[14] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "High-efficiency medical image encryption method based on 2D logistic-gaussian hyperchaotic map," Applied Mathematics and Computation, Vol. 442, 2023. https://doi.org/10.1016/j.amc.2022.127738

[15] P. Parida, C. Pradhan, X. -Z. Gao, D. S. Roy and R. K. Barik, "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," IEEE Access, Vol. 9, pp. 76191-76204, 2021. https://doi.org/10.1109/access.2021.3072075

[16] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," Optik, Vol. 272, 2023. https://doi.org/10.1016/j.ijleo.2022.170316

[17] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, and X. Tang, "A 3D model encryption scheme based on a cascaded chaotic system," Signal Processing, Vol. 202, 2023. https://doi.org/10.1016/j.sigpro.2022.108745

[18] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," Expert Systems with Applications, Vol. 213, Part B, 2023. https://doi.org/10.1016/j.eswa.2022.119074

[19] W. Song, C. Fu, Y. Zheng, M. Tie, J. Liu and J. Chen, "A parallel image encryption algorithm using intra bitplane scrambling," Mathematics and Computers in Simulation, Vol. 204, pp. 71-88, 2023. https://doi.org/10.1016/j.matcom.2022.07.029

[20] S. Yan, L. Li, B. Gu, Y. Cui, J. Wang and J. Song, "Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image," Integration, Vol. 88, pp. 203-221, 2023. https://doi.org/10.1016/j.vlsi.2022.10.002

[21] L. Zhu, D. Jiang, J. Ni, X. Wang, X. Rong and M. Ahmad "A visually secure image encryption scheme using adaptive-thresholding sparsification compression sensing model and newly-designed memristive chaotic map," Information Sciences, Vol. 607, pp. 1001-1022, 2022. https://doi.org/10.1016/j.ins.2022.06.011

[22] A. Javeed, T. Shah and A. Attaullah, "Lightweight secure image encryption scheme based on chaotic differential equation," Chinese Journal of Physics, Vol. 66, pp. 645-659, 2020. https://doi.org/10.1016/j.cjph.2020.04.008

[23] S. Bhowmik and S. Acharyya, "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm," Journal of Information Security and Applications, Vol. 72, 2023. https://doi.org/10.1016/j.jisa.2022.103391

[24] L. Liu, and J. Wang, "A cluster of 1D quadratic chaotic map and its applications in image encryption," Mathematics and Computers in Simulation, Vol. 204, pp. 89-114, 2023. https://doi.org/10.1016/j.matcom.2022.07.030

[25] S. Zhou, X. Wang and Y. Zhang, "Novel image encryption scheme based on chaotic signals with finite-precision error," Information Sciences, Vol. 621, pp. 782-798, 2023. https://doi.org/10.1016/j.ins.2022.11.104

[26] E. Setyaningsih, R. Wardoyo, and A. K. Sari, "Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution," Digital Communications and Networks, Vol. 6, Issue 4, pp. 486-503, 2020. https://doi.org/10.1016/j.dcan.2020.02.001

[27] A. S. Alanazi, "A dual layer secure data encryption and hiding scheme for color images using the three-dimensional chaotic map and Lah Transformation," IEEE Access, Vol. 9, pp. 26583-26592, 2021. https://doi.org/10.1109/access.2021.3058112

[28] W. J. Jun, and T. S. Fun, "A new image encryption algorithm based on single S-box and dynamic encryption step," IEEE Access, Vol. 9, pp. 120596-120612, 2021. https://doi.org/10.1109/access.2021.3108789

[29] M. Tanveer, T. Shah, A. Rehman, A. Ali, G. F. Siddiqui, T. Saba, and U. Tariq, "Multi-images encryption scheme based on 3D chaotic map and Substitution Box," IEEE Access, Vol. 9, pp. 73924-73937, 2021. https://doi.org/10.1109/access.2021.3081362

[30] Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, M. A. Al Sibahee, V. O. Nyangaresi, D. G. Honi, A. I. Abdulsada, and X. Jiao, "Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map," IEEE Access, Vol. 10, pp. 26257-26270, 2022. https://doi.org/10.1109/access.2022.3151174

[31] S. Deb, and P. K. Behera, "Design of key-dependent bijective S-boxes for color image cryptosystem," Optik, Vol. 253, 2022. https://doi.org/10.1016/j.ijleo.2021.168548

[32] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," Microprocessors and Microsystems, Vol. 65, pp. 1-6, 2019. https://doi.org/10.1016/j.micpro.2018.12.003

[33] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," IEEE Access, Vol. 9, pp. 61334-61345, 2021. https://doi.org/10.1109/access.2021.3073514

[34] J. A. Namuq, F. S. Hasan, and A. H. Ali, "Image encryption based on S-box and 3D-chaotic maps and secure image transmission through OFDM in Rayleigh Fading Channel," Engineering and Technology Journal, Vol. 42, Issue 2, pp. 288-297, 2024. https://doi.org/10.30684/etj.2024.141722.1508

[35] J. Wang, J. Chen, F. Wang, and R. Ni, "Optical Image Encryption scheme based on quantum S-box and meaningful ciphertext generation algorithm," Optics Communications, Vol. 525, 2022. https://doi.org/10.1016/j.optcom.2022.128834

[36] A. Zahid, and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," Symmetry, Vol. 11, Issue 3, 2019. https://doi.org/10.3390/sym11030437

[37] M. Aslam, S. Beg, A. Anjum, Z. Qadir, S. Khan, S. U. R. Malik, M. A. P. Mahmud, "A strong construction of S-box using Mandelbrot set an image encryption scheme," PeerJ Computer Science, Vol. 8, 2022. https://doi.org/10.7717/peerj-cs.892

[38] R. H. Sani, S. Behnia, and A. Akhshani, "Creation of S-box based on a hierarchy of julia sets: Image encryption approach," Multidimensional Systems and Signal Processing, Vol. 33, Issue 1, pp. 39-62, 2021. https://doi.org/10.1007/s11045-021-00786-9

[39] S. Ibrahim, and A. Alharbi, "Efficient Image Encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography," IEEE Access, Vol. 8, pp. 194289-194302, 2020. https://doi.org/10.1109/access.2020.3032403

[40] B. B. Cassal-Quiroga, and E. Campos-Cantón, "Generation of dynamical S-boxes for block ciphers via extended logistic map," Mathematical Problems in Engineering, Vol. 2020, pp. 1-12, 2020. https://doi.org/10.1155/2020/2702653

[41] S. Zhou, Y. Qiu, X. Wang, and Y. Zhang, "Novel image Cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box," Nonlinear Dynamics, Vol. 111, pp. 9571-9589, 2023. https://doi.org/10.1007/s11071-023-08312-1

[42] X.-Y. Wang, H.-H. Sun, and H. Gao, "An image encryption algorithm based on improved Baker transformation and chaotic S-box," Chinese Physics B, Vol. 30, Issue 6, 2021. https://doi.org/10.1088/1674-1056/abdea3

[43] 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, Issue 9-10, pp. 6135-6162, 2019. https://doi.org/10.1007/s11042-019-08282-w

[44] X. Wang, and J. Yang, "A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system," Optik, Vol. 217, 2020. https://doi.org/10.1016/j.ijleo.2020.164884

[45] L. Liu, and J. Wang, "A cluster of 1D quadratic chaotic map and its applications in image encryption," Mathematics and Computers in Simulation, Vol. 204, pp. 89-114, 2023. https://doi.org/10.1016/j.matcom.2022.07.030

[46] S. Bhowmik, and S. Acharyya, "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm," Journal of Information Security and Applications, Vol. 72, 2023. https://doi.org/10.1016/j.jisa.2022.103391

[47] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," Signal Processing, Vol. 168, 2020. https://doi.org/10.1016/j.sigpro.2019.107340

[48] X. Wang, Y. Su, M. Xu, H. Zhang, and Y. Zhang, "A new image encryption algorithm based on Latin square matrix," Nonlinear Dynamics, Vol. 107, Issue 1, pp. 1277-1293, 2021. https://doi.org/10.1007/s11071-021-07017-7

[49] L. Teng, X. Wang, and Y. Xian, "Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion," Information Sciences, Vol. 605, pp. 71-85, 2022. https://doi.org/10.1016/j.ins.2022.05.032