All Sciences Proceedings
http://as-proceeding.com/

1st International Conference on Trends in Advanced Research
March 4-7, 2023 : Konya, Turkey

ICTAR

A New Image Encryption Algorithm

Fırat Artuğer[1*]

[1] Department of Computer Engineering / Faculty of Engineering, Munzur University, Turkey

*(firatartuger@munzur.edu.tr)

Abstract **–** With today's developing technologies, the need for new image encryption algorithms is increasing. Image encryption algorithms based on S-box and chaotic structures are a very popular topic. In this study, a new image encryption algorithm is proposed using different s-box structures. In the proposed method, an s-box is first obtained by using a chaotic map. Then, zig-zag scanning method is applied to this s-box structure and a new s-box is obtained. With the new s-box obtained, XOR operation is applied to the first 256 pixels from the image. This data obtained later is mixed by passing through the s-box structure created with the chaotic map at the beginning. In this way, the encryption process is completed when all blocks of the image are processed.

Keywords – Image encryption, s-box, chaotic map, zig-zag scanning, XOR

I. INTRODUCTION

With today's developing technologies, ensuring the confidentiality of data has been one of the most important issues. Digital documents (text, images, etc.) are often used and transmitted over insecure networks. In addition to text data, more interactive image data are also frequently used [1]. At this point, encryption algorithms are used to ensure confidentiality. Many encryption algorithms have been developed from past to present. However, different algorithms are still needed according to the needs of the applications. Whether it is text or image encryption, the block cipher philosophy is generally used. Some of those; DES [2] is 3DES and today's standard AES [3] algorithm. In block cipher algorithms, data is divided into equal blocks. Then each block is encrypted in itself. The encrypted blocks are combined and encrypted data is obtained. The logic is the same for encrypting images. Image data is split into pixels and encrypted in blocks. Chaotic systems are often used in encryption and they are quite efficient. Due to the nature of chaos, randomness provides many advantages for cryptographic structures. Similarly, s-box structures are one of the most important structures used in block cipher algorithms to mix data [4].

S-box structures, in other words, substitution boxes, allow one value to be replaced by another value. Since they perform this process in a non-linear way, they make it difficult for attackers to make inferences. Chaos is also frequently used in the production of S-box structures. Thanks to a chaotic map, an s-box can be easily obtained. Some of the studies that performed the image encryption process using chaos, s-box, or other structures are mentioned below.

A new two-dimensional chaotic map and a new method based on s-box structures are proposed for image encryption. The s-box structures obtained in this method were obtained with the chaotic map proposed in the study [5]. A new method based on DNA computation and chaos-based s-box structures has been developed to encode color images [6]. A new image encryption algorithm based on S-box has been developed. The s-box structures developed in this method were obtained by mathematical transformations. In this way, nonlinearity values are quite high [7]. A new image encryption scheme based on chaotic map and cuckoo search optimization was created. In this study, the s-box was improved and the nonlinearity value was increased by optimization [8]. A new image encryption scheme was created using the cellular automata, s-box, and Lorenz system [9]. A new image encryption algorithm is proposed using chaotic systems, optimization algorithms, and PUF structures [10].

II. PROPOSED METHOD

In this study, a new image encryption scheme was created using new s-box structures. First, a random s-box structure is created using the chaotic Lorenz system. The mathematical model of the chaotic Lorenz system is given in equation 1.

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (bx - y - xz) \\ \frac{dz}{dt} = (xy - cz) \end{cases} \tag{1}$$

The value obtained by equation 1 is converted to an integer and the mod256 operation is applied. If this value is not present in the s-box, it is added, if any, a new value is generated and the process continues. In this way, when 256 cells are filled, a chaotic s-box structure is obtained. Then, a new s-box is obtained by applying the zig-zag scanning method to this chaotic s-box structure. The basic structure of the zig-zag scanning method is given in figure 1.

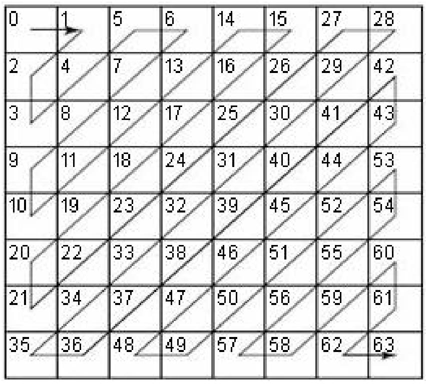

Figure 1. Zig-zag scanning method

A new and generally stronger s-box is obtained by passing the chaotic s-box structure through the scanning method given in figure 1. The zig-zag scanning method has been used before and it has been found to increase the performance of s-box structures at high rates [11]. With the s-box structure obtained because of scanning, 256 pixels of the original image are XORed. Then the values from here are finally passed through the chaotic s-box structure obtained at the beginning. This continues until all blocks of the image have been processed. After all blocks are passed through these processes, an encrypted image is obtained. The flow chart of the proposed algorithm is given in Figure 2.

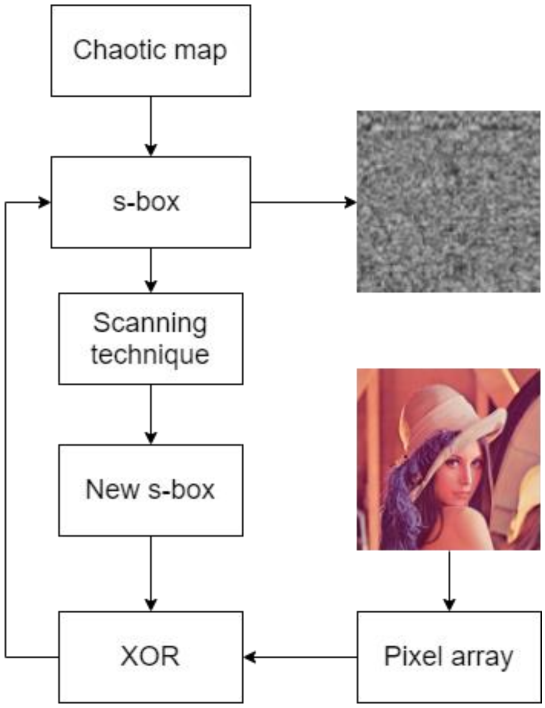

Figure 2. Flow chart of the proposed image encryption algorithm

III. S-BOX ANALYSIS RESULTS

The s-box structure obtained with the chaotic Lorenz system is given in Table 1. S-box is a nonlinear structure and this value is expected to be high. The nonlinearity value of the s-box structure obtained with the chaotic Lorenz map was calculated as 102.5. This value is low. The most important disadvantage of s-box structures obtained with chaotic maps is that these values are low. Various methods exist to improve such structures. Zig-zag scanning method is one of them. The s-box structure obtained after scanning the initial chaotic map with the zig-zag scanning method is given in Table 2. In this s-box, the nonlinearity value increased to 104. Thanks to this value, more effective mixing will be achieved in the proposed method. To evaluate an s-box; strict avalanche criterion, bit independence criterion, bijectivity, input-output XOR distribution values are frequently used. The s-box structures obtained in this study also meet these criteria. However, this study focused on the nonlinearity criterion. Because scanning methods such as zig-zag generally increase the nonlinearity value of s-box structures. Other criteria do not change much with such methods. In addition, since each value between 0 and 256 is used only once in the obtained s-box structures, they also provide the bijectivity feature.

Table 1. S-box obtained with the chaotic map

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

Table 2. S-box obtained after zig-zag scanning

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

IV. CONCLUSION

In this study, a new image encryption algorithm is proposed. This algorithm is based on chaotic Lorenz system and s-box structures based on zig-zag scanning. In the proposed algorithm, an s-box is obtained with the chaotic map. A new s-box structure is obtained by passing this s-box through the zig-zag scanning method. A block of the image is divided into blocks and the s-box obtained after scanning is passed through the XOR function. Then the obtained value is mixed by passing through the s-box structure obtained with the chaotic map. In this way, when all blocks are completed, an encrypted image is obtained. Decrypting the image is again quite simple. When the given operations are applied in reverse, the image will be decrypted. For this, the inverse of the proposed s-box structures should be taken. In addition, there are many scanning methods in the literature. It is thought that more effective s-box structures can be obtained by using different scanning techniques.

REFERENCES

[1] Gao, X., Mou, J., Xiong, L., Sha, Y., Yan, H., & Cao, Y. (2022). A fast and efficient multiple images encryption

based on single-channel encryption and chaotic system. Nonlinear Dynamics, 108(1), 613-636.
[2] Standard, D. E. (1999). Data encryption standard. Federal Information Processing Standards Publication, 112.
[3] J. Daemen and V. Rijmen, ''AES proposal: Rijndael,'' in Proc. 1st Adv. Encryption Conf., CA, USA, 1998, pp. 1–45.
[4] Artuğer, F., & Özkaynak, F. (2021). An effective method to improve nonlinearity value of substitution boxes based on random selection. Information Sciences, 576, 577-588.
[5] Zhou, S., Qiu, Y., Wang, X., & Zhang, Y. (2023). Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. Nonlinear Dynamics, 1-19.
[6] Masood, F., Masood, J., Zhang, L., Jamal, S. S., Boulila, W., Rehman, S. U., ... & Ahmad, J. (2021). A new color image encryption technique using DNA computing and Chaos-based substitution box. Soft Computing, 1-17.
[7] Razaq, A., Akhter, S., Yousaf, A., Shuaib, U., & Ahmad, M. (2022). A group theoretic construction of highly nonlinear substitution box and its applications in image encryption. Multimedia Tools and Applications, 1-22.
[8] Khan, H., Jamal, S. S., Hazzazi, M. M., Khan, M., & Hussain, I. (2023). New image encryption scheme based on Arnold map and cuckoo search optimization algorithm. Multimedia Tools and Applications, 82(5), 7419-7441.
[9] Alexan, W., ElBeltagy, M., & Aboshousha, A. (2022). Rgb image encryption through cellular automata, s-box and the lorenz system. Symmetry, 14(3), 443.
[10] Muhammad, A. U. S., & Özkaynak, F. (2021). SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs. Symmetry, 13(5), 824.
[11] Artuğer, F., & Özkaynak, F. (2020). A novel method for performance improvement of chaos-based substitution boxes. Symmetry, 12(4), 571.