symmetry

MDPI

Article

A Novel Method for Performance Improvement of Chaos-Based Substitution Boxes

Fırat Artuğer [1] and Fatih Özkaynak [2,*]

[1] Department of Computer Engineering, Faculty of Engineering, Munzur University, Tunceli 62000, Turkey; firatartuger@munzur.edu.tr

[2] Department of Software Engineering, Faculty of Technology, Fırat University, Elazığ 23119, Turkey

* Correspondence: ozkaynak@firat.edu.tr; Tel.: +90-424-237-0000

Received: 22 February 2020; Accepted: 16 March 2020; Published: 5 April 2020

Abstract: Symmetry plays an important role in nonlinear system theory. In particular, it offers several methods by which to understand and model the chaotic behavior of mathematical, physical and biological systems. This study examines chaotic behavior in the field of information security. A novel method is proposed to improve the performance of chaos-based substitution box structures. Substitution box structures have a special role in block cipher algorithms, since they are the only nonlinear components in substitution permutation network architectures. However, the substitution box structures used in modern block encryption algorithms contain various vulnerabilities to side-channel attacks. Recent studies have shown that chaos-based designs can offer a variety of opportunities to prevent side-channel attacks. However, the problem of chaos-based designs is that substitution box performance criteria are worse than designs based on mathematical transformation. In this study, a postprocessing algorithm is proposed to improve the performance of chaos-based designs. The analysis results show that the proposed method can improve the performance criteria. The importance of these results is that chaos-based designs may offer opportunities for other practical applications in addition to the prevention of side-channel attacks.

Keywords: chaos; cryptography; substitution box; postprocessing

1. Introduction

Developments in Industry 4.0, the Internet of Things (IoT) and artificial intelligence have changed our lives significantly. Although these changes make our lives easier in many ways, guaranteeing the security of the huge quantities information called big data is a serious problem. Strong cryptographic protocols are needed to address this problem. However, cryptology is a complex discipline. It is not enough to demonstrate that only certain security requirements are met. New methods and countermeasures should be constantly researched as new attack techniques are developed [1,2]. Application attacks are an important cryptanalysis technique that threatens existing encryption protocols [3]. One of the attack techniques, called side-channel analysis, is based on the principle of obtaining the secret key of the algorithm with the help of measurements such as sound, heat, light and power consumption after the encryption protocol is implemented on hardware such as a computer, mobile phones or FPGA cards.

Recent studies have shown that chaos-based encryption protocols may be more resistant to side-channel attacks than encryption protocols based on mathematical techniques. In the analysis carried out in [4], first, a side-channel analysis of the AES block encryption algorithm was performed. In the second stage of the analysis, a side-channel analysis of the AES block encryption algorithm was performed using chaotic substitution box (s-box) structures instead of the s-box structure based on mathematical methods proposed by Nyberg [5,6]. The second design is more resistant to side-channel

attacks than the standard AES algorithm. In other words, chaos-based s-box structures are more resistant to side-channel attacks than the AES s-box structure, which has the best-known s-box design criteria. However, when a literature review was undertaken, it was shown that even chaos-based designs with the best s-box performance criteria were worse than the Nyberg s-box structure. For example, for nonlinearity measurements, which play an important role in confusion and diffusion requirements, the best achievable value in chaos-based designs is 106.75, while in the Nyberg s-box structure, that value is 112, which is the upper bound value that can be reached [7].

It is therefore possible for chaos-based designs to be more resistant to side-channel attacks than mathematical designs. However, the poor performance criteria for these designs are an important problem. This study seeks to address this problem. Various studies have been published showing that the performance criteria can be improved with the help of optimization algorithms. However, in these approaches, there is another design problem, i.e., the additional processing cost of optimization algorithms. In this study, it has been shown that s-box performance criteria can be improved by applying various postprocessing techniques to chaos-based s-box designs. The practical applicability of the proposed method, its simple structure, and the speed of producing results have been evaluated as the advantages of the proposed method. This also raised a new research question regarding how s-box structures with better performance criteria can be obtained by using different postprocessing techniques in the future.

The rest of the study is organized as follows. In Section 2, the general design principle of chaos-based s-box structures and the basic milestones related to the literature are explained. In Section 3, the details of the proposed postprocessing technique are presented to improve the s-box performance criteria. In Section 4, the success of the proposed method is tested by providing various analysis results. The obtained results are interpreted and a road map for future studies is presented in Section 5.

2. Chaos-Based S-Box Structures

Chaos theory offers researchers various opportunities in many areas of science [8]. The rich dynamics that it contains have always made chaotic systems a popular research area. In addition to its use in modeling and control areas, its random behavior has led cryptography experts to focus on this field [9]. The basic idea behind this interest is that confusion and diffusion requirements can be met with the principle of sensitive dependence on initial conditions and control parameters. Confusion and diffusion requirements are two important properties of encryption protocols. These requirements were identified by Claude Shannon in 1945. "Confusion makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, most or all the bits in the ciphertext will be affected. Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change". It has been suggested that these requirements can be met using chaotic systems, since chaotic outputs are extremely sensitive to changes in initial conditions and control parameters, and have a nonlinear characteristic. Researchers have used chaotic systems as an entropy source in cryptographic designs. They used the initial condition and control parameters of chaotic systems as the secret key of cryptographic protocols. It has been suggested that different entropy sources can be produced by using different initial conditions and control parameters, as they will produce different outputs with small changes that may occur in the initial conditions and control parameters. Many cryptographic protocols such as image encryption algorithms [10,11], key generators [12,13] and s-box designs [14] have been proposed using this design idea, as visualized in Figure 1.

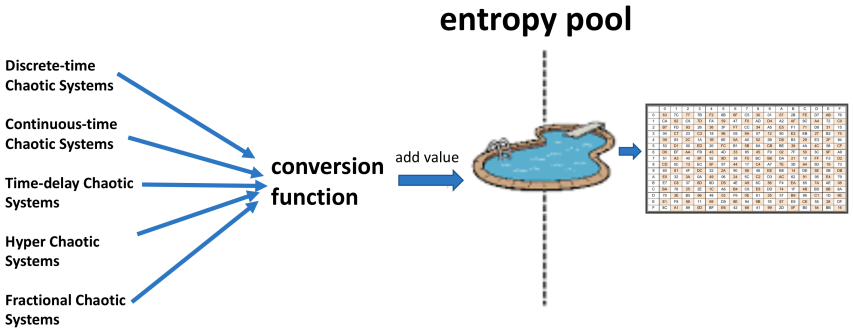

Figure 1. General design approach for chaos-based cryptographic protocol designs.

Although this design approach has been widely studied, the security analysis of some proposals has not been done according to certain criteria, which has caused various security problems. Chaos-based s-box designs stand out as a design class that is not affected by these problems, because the requirements for s-box performance analysis are almost standardized [15,16]. Bijective, nonlinearity, bit independence criterion (BIC), strict avalanche criterion (SAC) and input/output XOR distribution criteria are the standard measurements used in analysis processes of s-boxes. A nonlinearity criterion can be associated with the confusion criterion, which is one of the general characteristics of encryption algorithms; the ideal value for this criterion is 112, and the ideal value for the strict avalanche criterion is 0.5. This value indicates the difficulty of making statistical inferences. Values smaller or greater than 0.5 increase the success of statistical analysis. BIC measurement is related to nonlinearity and SAC measurements through the relationship between input and output bits. Input/output XOR distribution is related to differential cryptanalysis. To show its resistance against differential attacks, the maximum value that can be calculated. The expected value is 4; larger values indicate that differential attacks can be more successful [14–16].

In the simplest terms, s-box structures have the mathematical model given in Equation (1). In other words, it is a bijective function that converts values in a certain range to values in another range. The AES s-box structure is a nonlinear function that maps 256 values between 0 and 255 to 256 values between 0 and 255. Therefore, in the literature, attempts have been made to obtain different s-box structures by converting the chaotic system outputs to 256 different values. Many different s-box structures have been generated by changing the initial conditions and control parameters. Also, different chaotic system classes or different conversion algorithms have been used to improve the s-box performance criteria.

$$S: \begin{matrix} F_2^n \\ (x_1, \ldots, x_n) \end{matrix} \rightarrow \begin{matrix} F_2^m \\ (y_1, \ldots, y_m) \end{matrix} \quad (1)$$

When design studies are classified in terms of chaotic system types, there are two general classes: discrete and continuous-time chaotic systems. Discrete-time systems are among the preferred systems for researchers in the design process [17–21]. The main reason for this is that the systems can produce very fast results due to their simple mathematical models. The biggest advantage of continuous-time systems is that they have more complex mathematical models than discrete-time systems [22–26]. It is thought that this complexity will positively affect the quality of the entropy source. To use this advantage of continuous-time systems most effectively, special chaotic systems such as hyperchaotic [27,28], time-delay [29,30] and fractional-order systems [31,32] have also been used in the design process.

Another remarkable element of the general design architecture visualized in Figure 1 is the conversion function. The purpose of this function is to convert chaotic system outputs into an entropy source. In the literature, two conversion functions are most common. The first is the threshold value function. As stated in Equation (2), the chaotic system outputs are converted to 0 or 1 values by comparing them with a threshold value. Choosing the appropriate threshold value is a critical design

problem. It has been shown that successful results can be obtained if 0.5 is selected as the threshold value in many sources [33,34]. The other conversion function is the mode function. It has been shown in various studies that the mode function has various advantages, since it is a one-way function which guarantees various statistical properties [35–37]. Due to these advantages, in the proposed method, the mode function has been used to transform the chaotic entropy source into s-box structures.

$$f_{threshold}(x) : \begin{cases} 0 & x \leq 0.5 \\ 1 & x > 0.5 \end{cases} \tag{2}$$

3. Detail of Proposed Method

Block encryption algorithms are ineffective in the encryption of digital images. One of the most important reasons for this problem is the high correlation between the pixel values of an image [38]. Usually, images are represented by a matrix with a size of $m \times n$. The values of m and n indicate the values of the row and column, respectively. One of the proposed approaches to solving the correlation problem is to reposition the matrix cells using the zigzag transformation method, as shown in Figure 2. In this study, we propose the use of the zigzag reading approach as a postprocessing technique.

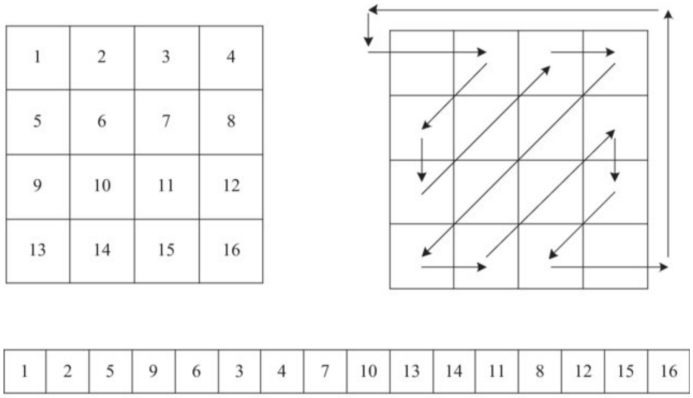

Figure 2. General structure of zigzag transformation approach.

Since AES-like s-box designs comprise a matrix with a size of 16 × 16, the zigzag transformation approach can be easily performed. The flowchart of the proposed method is given in Figure 3. The operation of the algorithm is given step by step below. Also, the pseudo code is expressed in Table 1 for the logistic map.

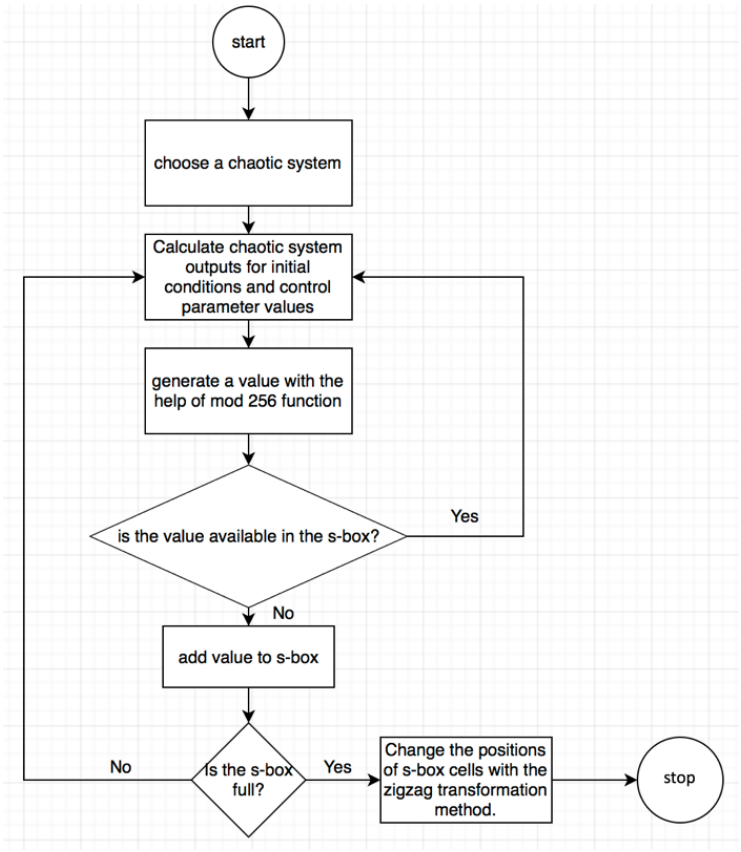

Figure 3. Flowchart of the proposed method.

Step 1. A discrete or continuous time chaotic system is chosen.

Step 2. The initial condition and control parameter values in which the chaotic system can exhibit rich random features are determined.

Step 3. State variable(s) of the chaotic system are calculated. Preferably, the first 1000 values can be ignored to eliminate the effects of transient response.

Step 4. The status variable value, which is the fractional value, is converted to a decimal value between 0–255 by applying mod 256.

Step 5. If the decimal value is not included in the s-box, it is added, otherwise a new state variable value is calculated, which continues until the table is full.

Step 6. The positions of s-box cells are shuffled using zigzag transformation.

Table 1. The pseudo code of chaotic s-box generation.

```
ChaoticSboxGenerate()
begin

sbox=[0:255]
for(k=0;k<256;I++)
sbox[k]=-1
end for

xOld= Random_Selection [0,1]

for(i=0;I<1000;I++)
xNew=4*xOld*(1-xOld)
xOld=xNex
end for

j=0;
while (j<sbox.lenght)
value=(xNex*100000000)%256
if(!contain(sbox,value))
sbox[j]=value
j++;
end if
xNew=r*xOld*(1-xOld)
xOld=xNex
end while

return ZigZagTransform(sbox)
end

contain(array, value)
begin
for(int i=0;i<array.length;i++)
if(array[i]==value)
return true
end if
end for
return false
end
```

4. Performance Analysis of Proposed Method

The study is based on a general s-box generator algorithm to examine the effect of the proposed postprocessing technique on the s-box performance. A flowchart of the s-box generator algorithm is given in Figure 3. The details of this algorithm and the program prepared for the Windows operating system can be accessed from [7,14]. Researchers can generate s-box structures using the original method, and verify their performance improvements for new s-box structures modified using the postprocessing technique through the program in [14].

The effect of the proposed method on the performance criteria was analyzed in this section. As explained, there are five basic criteria for s-box performance analysis. The bijective criterion is guaranteed by the proposed method. Therefore, this criterion is not included in the analysis tables. Two main categories can be used to classify chaotic systems. These categories are discrete and continuous-time chaotic systems. Discrete-time systems are first-order difference equations. Continuous-time chaotic systems are at least third-order differential equations [8]. An analysis of six different chaotic systems was carried out using three different chaotic systems for both chaotic system classes. Twenty-five different s-box structures were generated for each chaotic system class. Logistic

map, sine map, and circle map are used as discrete-time chaotic systems. Performance comparisons for original and improvement s-box structures are given in Tables 2–4 respectively. Similarly, performance comparisons for the original and improved s-box structures generated for each of the continuous-time Lorenz, Labyrinth Rene Thomas system, and Chua systems are given in Tables 5–7, respectively. To show the success of the proposed method, care was taken to ensure that the average nonlinearity property of all the original s-box structures used in the analysis was less than 103. Performance improvement was observed in all the s-box structures given in the analysis tables.

Table 2. Performance comparisons for original and improved s-boxes based on a logistic map.

	Performance Criteria for Original S-box					Performance Criteria for Improved S-box				
Name.	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**
L.map_1	100.75	0.4971	102.71	0.4992	12	105	0.5046	103.64	0.5009	10
L.map_2	102.5	0.5051	104.86	0.5012	12	103	0.5056	102.93	0.5004	12
L.map_3	102.75	0.502	103.21	0.5022	12	104.5	0.5027	102.93	0.4983	12
L.map_4	103.5	0.4985	104.29	0.4981	10	104.75	0.5049	103.71	0.4979	10
L.map_5	101.75	0.4998	103.21	0.4996	10	104.5	0.4983	103.64	0.5011	12
L.map_6	103.25	0.4976	103.64	0.4968	10	103.75	0.4973	103.29	0.5013	12
L.map_7	102	0.5051	103.07	0.5017	12	104.25	0.491	103.64	0.501	12
L.map_8	101.25	0.5056	103.29	0.503	12	103.75	0.4934	103.86	0.4962	12
L.map_9	103.75	0.5059	102.64	0.4997	10	104.5	0.4907	103.86	0.4978	10
L.map_10	103	0.5015	104.71	0.5023	12	104.5	0.498	103.5	0.5018	10
L.map_11	103.5	0.5012	103.36	0.4999	10	104	0.4998	104.14	0.5018	12
L.map_12	103.25	0.5049	103.64	0.4948	10	103.5	0.5	102.36	0.4978	12
L.map_13	102.25	0.5042	103.64	0.503	12	103.25	0.5022	104.07	0.4963	10
L.map_14	102	0.512	103.36	0.4969	12	103	0.4971	102.86	0.5007	12
L.map_15	102.75	0.5007	103.86	0.5001	10	103.25	0.5088	104	0.5005	12
L.map_16	101	0.5039	103.07	0.4976	10	103.5	0.5005	102.86	0.4974	12
L.map_17	102.5	0.5134	102.86	0.5	10	103.5	0.5056	104.29	0.4978	10
L.map_18	103.5	0.499	103.64	0.4941	12	103.75	0.5161	103.64	0.4957	10
L.map_19	102.75	0.5073	102.93	0.5037	12	103.75	0.5002	102.5	0.5018	10
L.map_20	103.25	0.491	103	0.4951	10	104	0.5042	103,5	0.4993	10
L.map_21	102.5	0.5078	102.86	0.4985	10	103.75	0.5154	103.64	0.5013	14
L.map_22	102.75	0.4966	103.71	0.4997	10	103.75	0.5066	103	0.4973	12
L.map_23	102.25	0.5012	103.5	0.5015	12	103.25	0.5044	103.36	0.5022	12
L.map_24	102.5	0.5068	104.36	0.4986	12	104.25	0.511	104.21	0.5006	10
L.map_25	103.25	0.5012	103.29	0.4992	12	104.24	0.5071	104.71	0.5027	10

Table 3. Performance comparisons for original and improved s-boxes based on a sine map.

	Performance Criteria for Original S-box					Performance Criteria for Improved S-box				
Name.	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**
S.map_1	101.75	0.5122	104.07	0.4985	14	103.5	0.4924	103.64	0.4911	12
S.map _2	103	0.5046	102.86	0.4964	12	104.5	0.5027	103.64	0.4977	10
S.map _3	102.25	0.4988	102.5	0.498	12	104.25	0.4978	103.93	0.5017	12
S.map _4	103	0.5063	103.79	0.5029	12	104.5	0.5034	103.43	0.5013	12
S.map _5	103.25	0.4973	103.57	0.4978	12	104.5	0.51	103.93	0.5006	12
S.map _6	102.5	0.51	104	0.4967	12	103	0.511	103.64	0.4921	10
S.map _7	103.5	0.501	102.79	0.4991	12	103.75	0.5093	103.5	0.504	10
S.map _8	102.5	0.5002	104.07	0.5005	12	105	0.5083	103.79	0.5029	10
S.map _9	103.75	0.5002	103.57	0.495	12	104	0.5103	103	0.4988	12
S.map _10	101.5	0.4973	103.57	0.4981	10	103.25	0.4934	104	0.499	12
S.map _11	103.75	0.4934	104.29	0.4999	12	104.5	0.5083	104.5	0.4952	12
S.map _12	102	0.5054	103	0.4963	12	103	0.5103	103.43	0.4963	12
S.map _13	102.5	0.4993	104.29	0.4967	14	103.75	0.4971	103	0.501	12
S.map _14	101.5	0.5007	103.64	0.501	10	102.5	0.5056	104.14	0.5003	10
S.map _15	102	0.499	103.71	0.5003	12	102.75	0.498	103.71	0.4957	12
S.map _16	103	0.5002	104.07	0.5026	12	130.25	0.5166	103	0.4925	12
S.map _17	101.75	0.4973	102.86	0.4995	12	102	0.4961	103.43	0.4998	10
S.map _18	103	0.5022	103.07	0.4972	10	103.5	0.4988	103.14	0.499	10
S.map _19	102.75	0.4978	103.43	0.4998	10	104.75	0.4976	103.07	0.5005	12
S.map _20	103.25	0.4973	103.21	0.4959	12	104.75	0.501	103.86	0.5013	12
S.map _21	102.25	0.4934	103.21	0.4978	10	104.5	0.4998	104.14	0.5029	12
S.map _22	103.25	0.5017	102.86	0.4987	12	105	0.5029	105.07	0.5017	10
S.map _23	103	0.5012	103.57	0.5014	12	103.75	0.5107	104.36	0.4997	12
S.map _24	103	0.5078	103.71	0.4994	10	103.75	0.5059	104	0.5007	10
S.map _25	102.75	0.5044	103.14	0.5009	10	103.25	0.5005	103.29	0.5021	12

Table 4. Performance comparisons for original and improved s-boxes based on a circle map.

	Performance Criteria for Original S-box					Performance Criteria for Improved S-box				
Name.	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**
C.map_1	102.25	0.5098	102.93	0.495	12	104.25	0.5015	102.79	0.5031	10
C.map_2	103.5	0.5027	103.29	0.501	10	105.5	0.5042	103.64	0.5055	10
C.map_3	102.75	0.5029	104.14	0.4902	12	105.75	0.5005	103.07	0.495	10
C.map_4	103.5	0.4915	103.43	0.4973	10	104.25	0.5005	102.86	0.4974	10
C.map_5	102	0.5115	103.57	0.4965	12	102.5	0.5007	104.07	0.501	12
C.map_6	103.25	0.5105	102.93	0.5022	12	104.5	0.4917	103.29	0.4988	10
C.map_7	102.25	0.498	102.93	0.5024	12	104.25	0.502	103.64	0.4983	12
C.map_8	100.75	0.4998	104.07	0.4961	12	105	0.4954	103.71	0.5026	12
C.map_9	102	0.498	103.07	0.5009	12	102.75	0.5066	103.86	0.4977	10
C.map_10	103.25	0.4978	103.36	0.5017	12	103.5	0.5037	103	0.4986	14
C.map_11	103	0.4946	103	0.5034	14	104.25	0.5007	103.5	0.5004	12
C.map_12	103.5	0.4944	103.29	0.5019	12	105.25	0.4976	103.43	0.4946	10
C.map_13	103.5	0.4932	102.71	0.502	10	104	0.5	103.36	0.4957	12
C.map_14	103.25	0.5061	103.21	0.4982	10	105.5	0.5039	103.29	0.4995	10
C.map_15	102	0.4951	104.63	0.5052	10	104.25	0.5029	103.93	0.5015	10
C.map_16	102.25	0.4968	104	0.4957	10	104	0.5037	104.86	0.5044	10
C.map_17	102.75	0.4939	104.07	0.5012	10	104.5	0.4924	103.79	0.4971	12
C.map_18	102.75	0.5083	102	0.4979	10	103	0.5015	104.21	0.4983	10
C.map_19	103	0.51	103	0.5017	10	104.25	0.4978	103.71	0.4976	10
C.map_20	101.5	0.5078	103	0.5011	12	103.25	0.5034	102.5	0.5025	14
C.map_21	101.75	0.501	102.43	0.4977	10	102.25	0.4993	104	0.4992	10
C.map_22	102	0.5027	103	0.4925	10	102.25	0.5112	103.71	0.5014	10
C.map_23	103	0.4976	103.14	0.5002	10	103.75	0.4937	102.57	0.4995	14
C.map_24	102.75	0.4917	104.57	0.4983	10	103.75	0.4956	104.79	0.5004	12
C.map_25	101.75	0.5171	102.86	0.5014	12	104.75	0.5073	102.79	0.4966	10

Table 5. Performance comparisons for original and improved s-boxes based on a Lorenz system.

	Performance Criteria for Original S-box					Performance Criteria for Improved S-box				
Name.	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**
Lorenz_1	101.5	0.4902	103.64	0.4988	10	103.75	0.4973	103.21	0.5041	12
Lorenz _2	103.25	0.5044	103.29	0.5063	12	105	0.5037	102.79	0.4989	12
Lorenz _3	101.75	0.5063	103.36	0.4911	12	103	0.4998	103	0.4985	12
Lorenz _4	102.75	0.5042	103.5	0.5005	12	104.25	0.5027	103.21	0.5013	10
Lorenz _5	103.75	0.5095	104.86	0.4928	12	104.25	0.5024	103	0.5039	12
Lorenz _6	103.5	0.4944	103.79	0.5015	12	105.5	0.4937	104	0.4991	10
Lorenz _7	102.5	0.5027	103.21	0.4959	12	106.25	0.4929	104.07	0.499	14
Lorenz _8	102.25	0.4978	103.14	0.5002	14	103.25	0.4912	103.21	0.5029	12
Lorenz _9	102.25	0.4954	104.21	0.5	12	105.5	0.499	103.07	0.4957	12
Lorenz _10	103.25	0.5029	103.36	0.4959	12	103.75	0.5068	103.43	0.5028	12
Lorenz _11	101.5	0.5002	104.07	0.5018	10	103.75	0.4961	103.07	0.5036	12
Lorenz _12	101.25	0.5085	103.71	0.4981	10	103	0.5015	103.29	5033	12
Lorenz _13	101	0.5029	103.64	0.4989	10	105	0.5039	103.21	0.4993	12
Lorenz _14	102.75	0.4934	103.93	0.4938	12	104.5	0.4988	103.5	0.4992	12
Lorenz _15	103.25	0.4995	103	0.4996	10	103.5	0.4985	103.29	0.5045	10
Lorenz _16	103	0.4961	103.07	0.4987	14	103.25	0.5071	104.07	0.5008	12
Lorenz _17	103.75	0.5093	103.57	0.5015	12	104.25	0.4917	103.86	0.4958	14
Lorenz _18	102.75	0.5068	103.07	0.4994	10	103.25	0.4939	103.29	0.499	12
Lorenz _19	101.25	0.4998	102.79	0.5029	12	103	0.491	104.79	0.5029	10
Lorenz _20	103.25	0.5098	102.79	0.5015	10	104.25	0.499	103.57	0.4973	10
Lorenz _21	103.5	0.4973	103.21	0.4959	12	103.75	0.4971	102.71	0.4985	12
Lorenz _22	103.25	0.5046	103.21	0.4964	12	104.24	0.4988	103.29	0.4986	12
Lorenz _23	102.75	0.5017	103	0.504	12	103.75	0.5007	103.86	0.4991	12
Lorenz _24	103.5	0.5005	103.14	0.5007	10	103.75	0.4978	102.43	0.4964	12
Lorenz _25	102.75	0.5017	104.14	0.5003	12	105.5	0.4993	103.71	0.4993	12

Table 6. Performance comparisons for original and improved s-boxes based on the Labyrinth Rene Thomas system.

	Performance Criteria for Original S-box					Performance Criteria for Improved S-box				
Name.	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**
Thomas_1	101.75	0.5046	103.86	0.5018	10	103.5	0.4966	103.86	0.4997	10
Thomas _2	103.25	0.4993	103.29	0.4995	10	104.5	0.4932	103.07	0.4971	12
Thomas _3	102.5	0.5039	104.43	0.4937	12	104	0.5002	103.5	0.5022	12
Thomas _4	103.5	0.5132	104.07	0.4962	12	104	0.5032	102.93	0.4957	12
Thomas _5	102.5	0.5037	103.64	0.4982	12	104	0.5022	103.86	0.5033	14
Thomas _6	103.25	0.51	103.29	0.499	12	104.25	0.5015	103.36	0.4952	10
Thomas _7	103.25	0.4944	103.36	0.4967	12	104.25	0.5034	104.14	0.5047	10
Thomas _8	103	0.5054	102.93	0.502	12	104.75	0.5137	103.57	0.502	12
Thomas _9	103.25	0.4893	103.43	0.4962	12	105.25	0.5088	103.64	0.5017	12
Thomas _10	102	0.4963	104.07	0.4939	12	105.5	0.5095	103.71	0.4992	10
Thomas _11	103	0.5071	102.79	0.4975	10	104	0.502	103.29	0.496	10
Thomas _12	102	0.4976	104.71	0.4963	12	103	0.5149	103.43	0.5031	12
Thomas _13	102.25	0.5037	103.14	0.4941	10	103.5	0.5083	103.5	0.4999	10
Thomas _14	102.75	0.5	103.36	0.5001	10	103	0.4971	103.14	0.5008	12
Thomas _15	103.25	0.5117	102.29	0.4978	10	104	0.5063	104.07	0.4951	12
Thomas _16	103	0.5017	102.64	0.502	10	104	0.5105	103.86	0.5037	12
Thomas _17	101	0.4961	103.07	0.501	12	104.25	0.4897	103.86	0.498	10
Thomas _18	102.5	0.5056	103.86	0.4994	10	103.5	0.5078	103.57	0.5047	10
Thomas _19	103.5	0.4995	103.14	0.5017	10	103.75	0.4924	103.21	0.4967	14
Thomas _20	103	0.5078	103.5	0.4971	10	104.5	0.5012	104.07	0.5006	12
Thomas _21	103.25	0.5095	104	0.4996	12	104	0.5049	103	0.4983	10
Thomas _22	103	0.5027	104.14	0.5009	10	103.75	0.4998	104.21	0.5017	10
Thomas _23	102.5	0.5088	104	0.5021	12	104	0.5056	104.57	0.4983	10
Thomas _24	102.5	0.5051	104.14	0.4969	12	104.5	0.4998	103.5	0.498	10
Thomas _25	103.25	0.4983	102.86	0.5059	12	103.5	0.4951	103.79	0.5001	10

Table 7. Performance comparisons for original and improved s-boxes based on a Chua circuit.

	Performance Criteria for Original S-box					Performance Criteria for Improved S-box				
Name.	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**	**Average Nonlinearity**	**SAC**	**BIC-Non.**	**BIC-SAC**	**XOR**
Chua_1	103.75	0.4922	103.64	0.4988	14	104.25	0.5051	103.64	0.4999	10
Chua _2	103.75	0.4995	103.29	0.494	12	104.75	0.5078	104.21	0.4943	12
Chua _3	102.25	0.4939	103.79	0.506	12	105.5	0.5063	102.86	0.5001	12
Chua _4	103.25	0.5032	104.57	0.5054	10	105	0.51	103.21	0.5046	10
Chua _5	103.5	0.4954	103	0.5028	12	103.75	0.4956	103.5	0.4948	10
Chua _6	103.5	0.5034	103.29	0.502	12	104.25	0.5027	104	0.4973	10
Chua _7	103	0.5027	103.57	0.5024	12	103.75	0.5051	103.21	0.4995	12
Chua _8	102.5	0.5029	104.29	0.5015	10	104	0.5068	103.21	0.4994	10
Chua _9	102.75	0.5059	103.29	0.5011	10	105.25	0.5034	103.5	0.5009	12
Chua _10	103	0.4956	103.43	0.4958	12	104.5	0.5027	103.57	0.4986	12
Chua _11	102.75	0.5022	103.36	0.4971	12	104.25	0.4968	103.79	0.498	12
Chua _12	103.75	0.5039	103.43	0.4999	10	104.75	0.4976	104.07	0.5018	12
Chua _13	101.75	0.498	104.07	0.4981	12	104.75	0.4985	103.57	0.4993	12
Chua _14	102	0.5	103.64	0.4994	12	103.5	0.5024	104.29	0.502	12
Chua _15	102.5	0.5049	104	0.4994	10	103.5	0.5029	103.36	0.5037	12
Chua _16	103	0.4939	103.29	0.4993	14	104.25	0.5081	102.71	0.5006	10
Chua _17	103	0.5044	103.86	0.502	12	105.5	0.4998	103.57	0.4979	12
Chua _18	103	0.4922	103.64	0.5012	12	103.5	0.4983	102.29	0.4979	12
Chua _19	102.75	0.5034	104.57	0.4998	12	104.25	0.5	103.57	0.4931	10
Chua _20	103.25	0.5056	103.79	0.4992	12	103.5	0.4922	102.5	0.4976	12
Chua _21	102.25	0.5007	103.14	0.5065	12	103.5	0.4956	103.07	0.4956	14
Chua _22	103.25	0.4917	103.36	0.4985	10	105	0.5088	103.5	0.4937	12
Chua _23	101.25	0.4995	103.36	0.493	12	103.75	0.4915	103.29	0.4992	12
Chua _24	103	0.5103	102.79	0.4929	14	104.5	0.5007	103.64	0.5042	10
Chua _25	102.75	0.499	103.57	0.4985	12	103.25	0.5034	103	0.5013	12

The statistical properties of the chaotic data used in the s-box generation process are not included in this section. In [35], it is shown that the performance criteria of the s-box structures to be generated using the data which do not show chaotic behavior may be better than the s-box structures generated from chaotic data. In addition, in the code given in Table 1, the initial condition of the logistic map used as the chaotic system was chosen randomly. In other words, the proposed method provides performance improvement, regardless of the statistical properties of the entropy source. This is another strength of the proposed method.

5. Conclusions

Chaotic systems will provide various opportunities for cryptology sciences. Among these, a successful design approach is chaos-based s-box designs. However, the fact that chaos-based s-boxes are worse in terms of performance criteria than designs based on mathematical transformations is a serious problem. This problem is addressed in the study. The question of whether performance improvements of chaos-based designs can be achieved using various postprocessing methods was explored. In the study, the zigzag transformation method, which has a very simple structure, was used. It was observed that the proposed method provides performance improvements in chaos-based s-box structures that have performance characteristics that can be evaluated below average. Since the performance criteria of the chaos-based s-box structures are very close to each other, comparisons were made using the nonlinearity measurement, which is a criterion that can reflect the difference in the best way. In a literature review for the s-box, it was observed that the average value for the nonlinearity value is 103. Therefore, care was taken to ensure that the average nonlinearity value of all the s-box values used in the analysis was below 103. In line with these conditions, 150 different s-box structures were generated. The generated s-box structures were obtained from six different chaotic systems selected from two different chaotic system classes. The reason for using different chaotic systems was to show that the proposed method can be successful for all chaotic systems. All these s-box structures are explicitly presented for the examination of other researchers on a web page [39].

If a general evaluation is made, the advantages of the proposed method are listed below.

- It has been shown that s-box performance criteria can be improved using a postprocessing algorithm.
- The proposed postprocessing algorithm for performance improvements has a simple and elegant structure.
- Speed, computational complexity, and user friendliness are strong features of the proposed method.
- Considering these advantages, it can be said that the proposed postprocessing algorithm is a more convenient method for performance improvement compared to the optimization algorithms described in the literature to date.
- The proposed method can give successful results, regardless of the chaotic system type and class.
- Only the s-box generator should not be considered as the output of the study. It has been shown that new designs can be developed that can be used as a counter measurement to prevent side channel attacks.

Despite these advantages, the proposed postprocessing idea should be based on a more robust foundation in future studies. Some possible avenues for future studies are listed below.

- Many different postprocessing algorithms can be developed to achieve performance improvements. An example is the displacement of s-box rows or columns.
- In this study, postprocessing was applied to only one s-box generator. The success of the proposed method on different s-box generators should be evaluated.
- The postprocessing technique gives successful results for the nonlinearity criteria of 103 and below. However, the question of how performance improvements can be achieved for designs with better nonlinearity measurements should be investigated.
- The fact that the performance improvement is independent of the chaotic system type and class reveals that the proposed method can produce successful outputs from different entropy sources. Performance improvements will be investigated for s-box structures that will be designed in the future using different entropy sources.
- The practical applicability of chaos-based s-box structures in the field of information security should be investigated.
- Applications of the obtained outputs in different fields can be investigated, such as W-MSR-type resilient algorithms, to cope with attacks in complex networks [40,41].

Author Contributions: F.A. and F.Ö. Wrote and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: The authors gratefully thank to the Referee for the constructive comments and recommendations which definitely help to improve the readability and quality of the study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, C.; Zhang, Y.; Yong, E. When an attacker meets a cipher-image in 2018: A year in review. *J. Inf. Sec. Appl.* **2019**, *48*, 1–9. [CrossRef]
2. Özkaynak, F. Brief Review on Application of Nonlinear Dynamics in Image Encryption. *Nonlinear Dyn.* **2018**, *92*, 305–313. [CrossRef]
3. Cho, J.; Kim, T.; Kim, S.; Im, M.; Kim, T.; Shin, Y. Real-Time Detection for Cache Side Channel Attack using Performance Counter Monitor. *Appl. Sci.* **2020**, *10*, 984. [CrossRef]
4. Açıkkapı, M.S.; Özkaynak, F.; Özer, A.B. Side-channel Analysis of Chaos-based Substitution Box Structures. *IEEE Access* **2019**, 79030–79043. [CrossRef]
5. Nyberg, K. Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1994; Volume 765, pp. 55–64.

6. Daemen, J.; Rijmen, V. AES proposal: Rijndael. In Proceedings of the 1st Advanced Encryption Conference, Ventura, CA, USA, 20–22 August 1998; pp. 1–45.
7. Özkaynak, F. Construction of Robust Substitution Boxes Based on Chaotic Systems. *Neural Comp. Appl.* **2019**, *31*, 3317–3326. [CrossRef]
8. Strogatz, S. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering (Studies in Nonlinearity)*; Westview Press: Boulder, CO, USA, 2001.
9. Kocarev, L.; Lian, S. *Chaos Based Cryptography Theory Algorithms and Applications*; Springer: Berlin/Heidelberg, Germany, 2011.
10. Zhu, C.; Wang, G.; Sun, K. Cryptanalysis and Improvement on an Image Encryption Algorithm Design Using a Novel Chaos Based S-Box. *Symmetry* **2018**, *10*, 399. [CrossRef]
11. Zhang, X.; Wang, X. Multiple-Image Encryption Algorithm Based on the 3D Permutation Model and Chaotic System. *Symmetry* **2018**, *10*, 660. [CrossRef]
12. Ding, L.; Liu, C.; Zhang, Y.; Ding, Q. A New Lightweight Stream Cipher Based on Chaos. *Symmetry* **2019**, *11*, 853. [CrossRef]
13. Demir, K.; Ergün, S. An Analysis of Deterministic Chaos as an Entropy Source for Random Number Generators. *Entropy* **2018**, *20*, 957. [CrossRef]
14. Özkaynak, F. An Analysis and Generation Toolbox for Chaotic Substitution Boxes: A Case Study Based on Chaotic Labyrinth Rene Thomas System. *Iran. J. Sci. Tech. Trans. Elect. Eng.* **2020**, *44*, 89–98. [CrossRef]
15. Cusick, T.; Stanica, P. *Cryptographic Boolean Functions and Applications*; Elsevier: Amsterdam, The Netherlands, 2009.
16. Wu, C.; Feng, D. *Boolean Functions and Their Applications in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2016.
17. Ahmad, M. Random search based efficient chaotic substitution box design for image encryption. *Int. J. Rough Sets Data Anal.* **2018**, *5*, 131–147. [CrossRef]
18. Hussain, I.; Anees, A.; Al-Maadeed, T.A.; Mustafa, M.T. Construction of S-Box Based on Chaotic Map and Algebraic Structures. *Symmetry* **2019**, *11*, 351. [CrossRef]
19. Zahid, A.H.; Arshad, M.J. An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. *Symmetry* **2019**, *11*, 437. [CrossRef]
20. Zhu, S.; Wang, G.; Zhu, C. A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes. *Entropy* **2019**, *21*, 790. [CrossRef]
21. Liu, H.; Zhao, B.; Huang, L. Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling. *Entropy* **2019**, *21*, 343. [CrossRef]
22. Lai, Q.; Akgul, A.; Li, C.; Xu, G.; Çavuşoğlu, Ü. A New Chaotic System with Multiple Attractors: Dynamic Analysis, Circuit Realization and S-Box Design. *Entropy* **2018**, *20*, 12. [CrossRef]
23. Lu, Q.; Zhu, C.; Wang, G. A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. *Entropy* **2019**, *21*, 1004. [CrossRef]
24. Liu, L.; Zhang, Y.; Wang, X. A Novel Method for Constructing the S-Box Based on Spatiotemporal Chaotic Dynamics. *Appl. Sci.* **2018**, *8*, 2650. [CrossRef]
25. Wang, X.; Akgul, A.; Cavusoglu, U.; Pham, V.-T.; Vo Hoang, D.; Nguyen, X.Q. A Chaotic System with Infinite Equilibria and Its S-Box Constructing Application. *Appl. Sci.* **2018**, *8*, 2132. [CrossRef]
26. Wang, X.; Çavuşoğlu, Ü.; Kacar, S.; Akgul, A.; Pham, V.-T.; Jafari, S.; Alsaadi, F.E.; Nguyen, X.Q. S-Box Based Image Encryption Application Using a Chaotic System without Equilibrium. *Appl. Sci.* **2019**, *9*, 781. [CrossRef]
27. Al Solami, E.; Ahmad, M.; Volos, C.; Doja, M.N.; Beg, M.M.S. A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes. *Entropy* **2018**, *20*, 525. [CrossRef]
28. Islam, F.; Liu, G. Designing S-box based on 4D-4 wing hyperchaotic system. *3D Res.* **2017**, *8*, 9. [CrossRef]
29. Özkaynak, F.; Yavuz, S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* **2013**, *74*, 551–557. [CrossRef]
30. Khan, M.; Shah, T.; Batool, S.I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Comp. Appl.* **2016**, *27*, 677–685. [CrossRef]
31. Özkaynak, F.; Çelik, V.; Özer, A.B. A New S-Box Construction Method Based on the Fractional Order Chaotic Chen System. *Signal Image Video Proc.* **2017**, *11*, 659–664. [CrossRef]

32. Zahid, A.H.; Arshad, M.J.; Ahmad, M. A Novel Construction of Efficient Substitution-Boxes Using Cubic Fractional Transformation. *Entropy* **2019**, *21*, 245. [CrossRef]
33. Tanyıldızı, E.; Özkaynak, F. A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps. *IEEE Access* **2019**, 117829–117838. [CrossRef]
34. Anees, A.; Hussain, I. A Novel Method to Identify Initial Values of Chaotic Maps in Cybersecurity. *Symmetry* **2019**, *11*, 140. [CrossRef]
35. Özkaynak, F. On the Effect of Chaotic System in Performance Characteristics of Chaos Based S-box Designs. *Phys. A Stat. Mech. Appl.* **2020**, 124072. [CrossRef]
36. Stoyanova, B.; Ivanova, T. CHAOSA: Chaotic map based random number generator on Arduino platform. *AIP Conf. Proc.* **2019**, *2172*, 090001. [CrossRef]
37. Zhu, S.; Zhu, C.; Wang, W. A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256. *Entropy* **2018**, *20*, 716. [CrossRef]
38. Yang, C.-H.; Chien, Y.-S. FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm. *Symmetry* **2020**, *12*, 189. [CrossRef]
39. Available online: http://www.kriptarium.com/symmetry.html (accessed on 3 November 2019).
40. Shang, Y. Hybrid consensus for averager-copier-voter networks with non-rational agents. *Chaos Solitons Fractals* **2018**, *110*, 244–251. [CrossRef]
41. Shang, Y. Consensus of hybrid multi-agent systems with malicious nodes. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**. [CrossRef]