IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 13, 2020, accepted December 19, 2020, date of publication December 22, 2020,
date of current version January 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3046470

A Method to Determine the Most Suitable Initial Conditions of Chaotic Map in Statistical Randomness Applications

MEHMET ŞAHIN AÇIKKAPI[1] AND FATIH ÖZKAYNAK[2,3]
[1]Department of Computer Technologies, Munzur University, 62100 Tunceli, Turkey
[2]Department of Software Engineering, Fırat University, 23119 Elâziğ, Turkey
[3]Kriptarium Inc., 23200 Elâziğ, Turkey

Corresponding author: Fatih Özkaynak (fatih@kriptarium.com)

The work of Fatih Özkaynak was supported in part by The Scientific and Technological Research Council of Turkey under Grant 120E444.

ABSTRACT The processes and systems in the real world actually contain order and symmetry. Understanding these order and symmetrical behavior has been a common effort of scientists. Chaos theory has been an interesting topic to understand these order and symmetrical behavior. One of the most important reasons for this interest is the rich dynamics of chaotic systems. A remarkable application of these systems is statistical randomness. Especially in random number generator designs based on discrete time chaotic systems, an important design parameter affecting the success of the generator (statistical randomness properties) is the initial conditions of chaotic maps. Obtaining different initial conditions that will meet the statistical requirements is important in terms of generating different random number sequences. In order to determine the initial conditions, an algorithm that updates the initial conditions depending on the number of successful statistical tests is proposed. Although the proposed design approach is similar to a back propagation neural network, it has a unique design approach. The NIST SP 800-22 test suite has been used to analyze the statistical properties of the proposed generator. It is known that the NIST SP 800-22 test suite is a hypothesis test. Therefore, in order to show the success of the proposed method in the best way, various additional analysis studies have been carried out proving that the generator outputs have a uniform distribution. Using the proposed method, six different initial conditions have been determined that provide statistical random properties for the discrete-time chaotic systems known as logistic map and tent map. 1,000,000 bits have been generated using the obtained initial conditions. These bit values are then converted to decimal values between 0-15. It is observed that the obtained numbers have a uniform distribution. These outputs are thought to be applicable in many areas such as games, simulation, modeling, determination of optimization parameters and cryptology. It is shown in a practical application for cryptographic substitution-box designs to examine the success of the outputs.

INDEX TERMS Chaos, cryptography, deterministic random numbers, randomness, statistical tests, s-box.

I. INTRODUCTION

Curiosity is always at the center of scientific research. Humanity has wondered many things throughout history. The outputs of the questions their tried to answer appeared as important milestones of science and engineering. One of the most important questions that researchers focus on is to predict the future behavior of processes and systems. We wish to be able to predict the outcomes of many processes and systems in order to sustain our lives more easily, comfortably and with good quality. However, the random nature of these processes and systems is one of the most important problems that prevent researchers from making successful predictions [1].

One of the remarkable studies among these prediction studies was conducted by Edward Lorenz in 1963 [2]. Lorenz, a mathematician and meteorologist, designed a model using differential equations to predict the weather. However, while analyzing the model, he discovered that the behavior he originally defined as an error is actually a product of the internal

The associate editor coordinating the review of this manuscript and approving it for publication was Chao-Yang Chen.

dynamics of the system. This principle, defined as sensitive dependence on initial conditions and control parameters, later revealed a new branch of science that researchers base on to model real-world systems [1]. This branch of science, known as the chaos theory, has revealed that even systems with a mathematical model are sensitive to changes in the initial conditions and control parameters. This phenomenon, also known as the butterfly effect, has affected many branches of science since its inception. Chaos theory has many application area such as math, biology, economy and medicine. One of the successful applications of the subject is statistical randomness [3]. The idea that chaotic systems can be used as a powerful entropy source has been extensively researched in the literature and continues to be investigated. Chaotic systems have rich dynamics as an entropy source. However, one of the most important parameters affecting the randomness quality of entropy sources to be generated based on chaotic systems is the initial conditions and control parameters of the system. Very small changes in the initial conditions and control parameters can produce very different outputs. Therefore, the quality of entropy source will be affected the most from these choices. In other words, choosing the appropriate initial conditions is an important design problem in chaos-based randomness studies [4].

The aim of this study is to find a suitable solution for this design problem. However, the initial conditions of chaotic systems are shown in fractional numbers. Since there are an infinite number of fractional numbers, an infinite number of different initial conditions can be selected. An infinite number of initial conditions can generate an infinite number of entropy sources. But which initial condition is best suited for randomness? There is no direct answer to this question because the solution space of the problem is infinite. In this study, a method has been proposed to solve this difficult problem. In order to determine the convenient initial conditions, proposed algorithm update the firstly selected initial conditions depending on the number of successful statistical tests is proposed. Although the proposed design approach is similar to a back propagation artificial neural network, it has a unique design approach. The success of the obtained results has been confirmed through the NIST SP 800-22 randomness test suite, which is considered a standard analysis method. It is thought that the chaos-based entropy source, which is the output of the study, can be widely used in many applications that require statistical randomness.

The rest of the study is organized as follows. In the second section, the relationship between chaos and randomness is explained. Also, in this section, a short literature summary about chaos based randomness studies is tried to be given. In the third section, details of the proposed architecture are explained in order to obtain the suitable initial conditions. In the fourth section, a random number generator is designed using the obtained initial conditions with the help of the proposed architecture. Then randomness properties of this generator have been analyzed using NIST SP 800-22 tests. The success of the obtained random bit sequences in a practical application is tested in the fifth section. The results are interpreted and suggestions are made for future studies in the last section.

II. CHAOS AND RANDOMNESS

Randomness plays an important role in many applications. In games, the result is desired to be uniform distribution for the satisfaction of the players. In fact, gamblers are a very good statistician. Therefore, it is desired that the outputs thought to be random are statistically independent. Cryptology is another application area where randomness is critical [5], [6]. Statistical independence is necessary but not sufficient in this discipline where sensitive data should be anonymized. In addition to statistical randomness, the outputs must be unpredictable in the information security applications. Avalanche criterion, or avalanche effect, a critical design parameter in many cryptographic protocol designs, can be used to best describe this statistically independent and unpredictable behavior. This criterion is satisfied "if, whenever a single input bit is complemented, each of the output bits changes with a 50% probability." In other words, randomness needs different requirements for different applications. If a general classification is to be made, there are two basic requirements for randomness [7], [8]. These requirements are:

- The randomness source should show good statistical properties.
- The randomness source should be unpredictable.

There are two basic classes of random numbers associated with these two basic requirements. These classes are deterministic and true random number generators [7]–[9]. Since it is not appropriate to talk about the randomness of a value alone, a random number sequence is used to measure randomness. Therefore, the random number generator (RNG) term will be used for the rest of the study. Deterministic random number generators (DRNG) generate random number sequences with the help of an algorithm. Since the algorithms are well-defined, before or after of the sequence can be predicted using a portion of the random number sequence. Therefore, the important thing for DRNG is that the generator has good statistical properties.

True random number generators (TRNG) use a powerful entropy source for generating random number sequences. This entropy source is unpredictable. In other words, the second requirement of randomness is provided. However, the outputs of TRNG do not have good statistical properties [7]–[9]. Various suggestions have been made to solve statistical problems in TRNG designs, which have been made recently in the literature. These suggestions are commonly known as post-processing techniques. The most widely known examples of these post-processing techniques are Von Neumann corrector [10], H-function [11], and resilient functions [12]. The emergence of various problems, such as the low data rate and high energy consumption speed in these widely known techniques, led researchers to seek new alternatives. Among these studies, various alternatives such as using the chaotic entropy pool [13], sampling through chaotic systems [14], using s-box structures [15] and other hardware implementation [16]–[18] attract attention.

Both DRNG and TRNG have been designed based on chaotic systems. In chaos-based DRNG studies, the chaotic system have been first modeled by computer and outputs of chaotic system have been calculated using models [19]. These outputs have been converted to random number sequences with the help of various conversion functions. There are many suggestions in this design approach that use different chaotic systems and different conversion functions [20]–[23]. Electronic circuit simulations of chaotic systems are generally used in chaos based TRNG designs. Random number sequences have been obtained by creating a strong entropy source with unexpected situations that could not be controlled situation in the electronic circuit design and operation [24]–[26]. There are several chaos-based random number generators that adopt the hybrid design approach in the literature [27]–[29].

A DRNG design has been used in this study. In the study, discrete-time chaotic systems have been used as chaotic systems. The reason for choosing discrete-time chaotic systems are simple mathematical models. This simple structure positively affects the speed parameter, which is an important evaluation factor in generator design. Again, within the scope of the speed parameter, the threshold function is used as the conversion function. The mathematical expression of the threshold function is given in Eq. (1). The flowchart showing the detailed structure of the generator is given in Figure 1.

$$f_{\text{threshold}}(x) : x <= 0,5 \, ? \, 0 : 1 \qquad (1)$$

III. DETAILS OF PROPOSED ARCHITECTURE

Choosing the appropriate initial conditions is an important problem for researchers. Since the most prominent feature of chaotic systems is the sensitive dependence on the initial conditions [30]. In order to show the relationship between chaotic behavior and initial conditions, the bifurcation diagram of the logistic map is shown in Figure 2 [31], [32]. The mathematical model of the logistic map is given in Eq. (2). The simple structure of the system is related to the fact that it contains only one initial condition and one control parameter. It can be observed from the bifurcation diagram that the control parameter value should be between 3.5 and 4 in order to display chaotic behavior [32].

$$x_{n+1} = r^{*}x_{n}^{*}(1\text{-}x_{n}) \qquad (2)$$

The bifurcation diagram is a qualitative analysis method. In other words, an expert is required to interpret the results of the analysis. Although there are different methods to analyze the presence of chaotic behavior in a system, Lyapunov exponents have several advantages over others. Lyapunov exponents are a quantitative analysis method. Positive Lyapunov exponents overlap is associated with chaotic behavior. Figure 3 shows the Lyapunov exponents calculated for the logistic map [1], [31], [32].

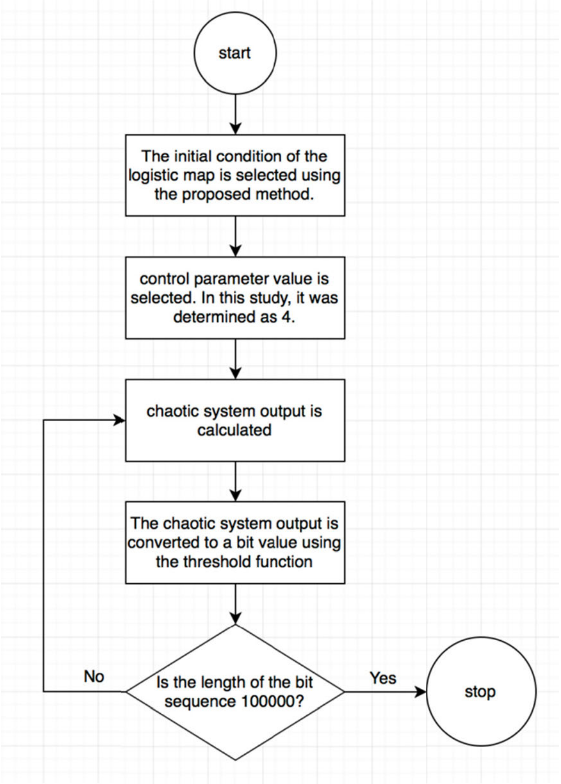
start
The initial condition of the logistic map is selected using the proposed method.
control parameter value is selected. In this study, it was determined as 4.
chaotic system output is calculated
The chaotic system output is converted to a bit value using the threshold function
Is the length of the bit sequence 100000?
No
Yes
stop

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

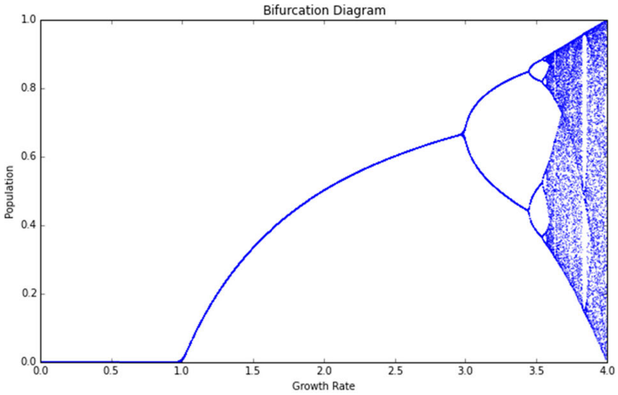

FIGURE 2. Bifurcation diagram of logistic map.

The analysis results which are carried out with both the bifurcation diagram and Lyapunov exponent of the logistic map show that the control parameter value of the system, which has the richest chaotic behavior, is 4. The question to be answered at this stage is what would be the most appropriate initial conditions to achieve the most appropriate statistical randomness using the method detailed in Figure 1? An architecture has been proposed to answer this question. Details of the proposed architecture are given in Figure 4. In order to determine the initial conditions, an algorithm that updates the initial conditions depending on the number of successful statistical tests is proposed. Although the proposed design

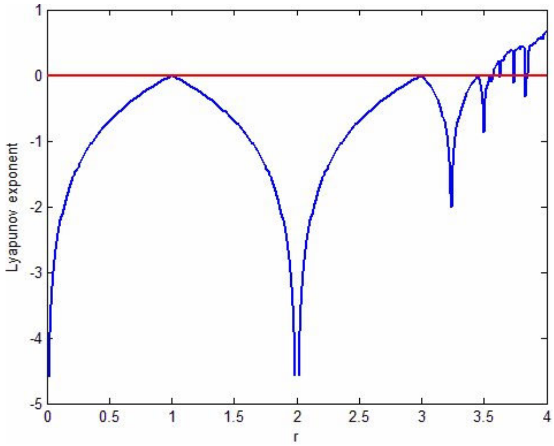

FIGURE 3. Lyapunov exponent diagram of logistic map.

approach is similar to a back propagation neural network, it has a unique design approach.

The proposed architecture is a three-layer back propagation architecture. There are two neurons in the input layer. There are 15 neurons in the middle layer of the neural network. Each neuron corresponds to one test in the NIST SP 800-22 test suite [33]. The initial values are updated depending on the number of successful tests. The starting point of this study is based on the proposed approach to determine the initial conditions with the help of optimization algorithms. In the proposed method in Ref. [34], the most appropriate initial condition and control parameters have been tried to be determined with the help of six different optimization algorithms. The initial condition of the logistic map is in the range of [0, 1]. So; there is an infinite number of possibilities to choose. The purpose of the proposed method in this study is to reduce the computational complexity of the previously proposed method. The method described below has been used to narrow the selection space containing the initial conditions.

Step 1. Firstly, [0.1; 0.3; 0.4; 0.7] are used as the initial condition.
Step 2. A digit value between 0-9 is generated using the rand() function.
Step 3. This digit value is added to the initial condition.
Step 4. Continue by selecting the digit value that provides the most test.
Step 5. Continue from step 2 until the number of digits after the comma reaches 15.

The obtained initial conditions using this architecture are given in Table 1.

Although the initial conditions listed in Table 1 have been obtained using the proposed method, it has been evaluated that there might be some defects of the method that needed improvement. Because in step 1 of the proposed algorithm an initial population has to be determined by the user. This choice can be interpreted as a disadvantage as it requires a user dependency. However, this disadvantage should be interpreted as a trade-off. Because determining the initial conditions with optimization algorithms is a process that takes weeks using an average computer (2,2 GHz Intel Core i7, 16 GB 1600 MHz DDR3). It took less than 5 minutes to obtain

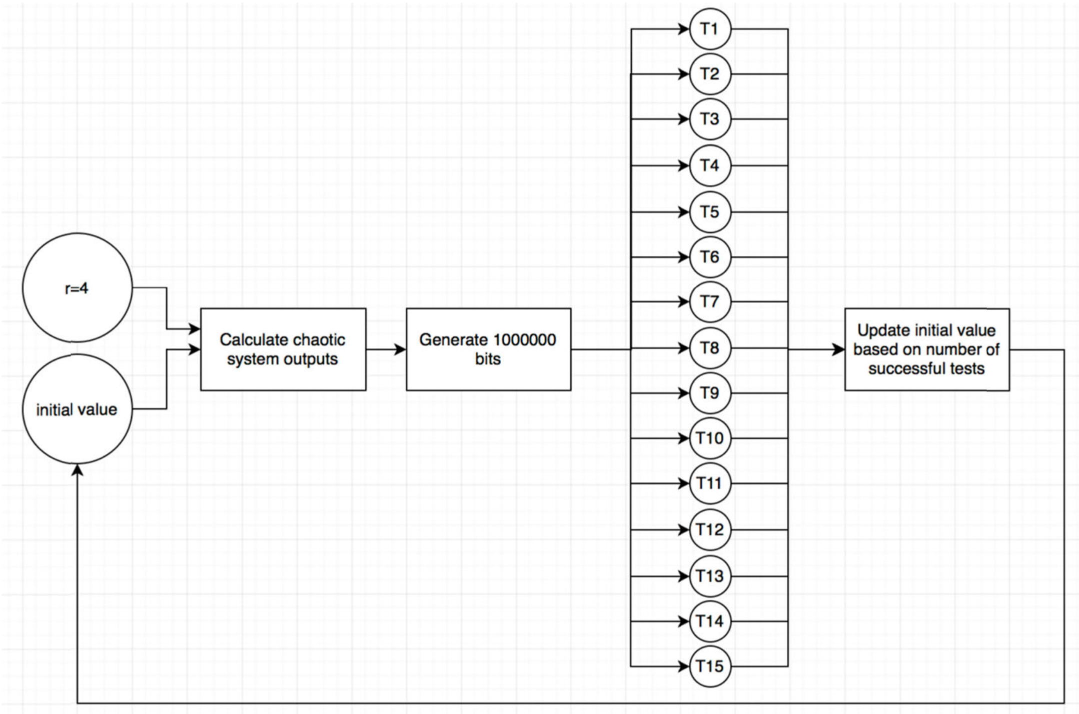
r=4
initial value
Calculate chaotic system outputs
Generate 1000000 bits
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
T14
T15
Update initial value based on number of successful tests

FIGURE 4. General overview of proposed architecture.

TABLE 1. The obtained initial conditions for logistic map.

Initial Conditions	value
value 1	0.187791210204038
value 2	0.306521897273215
value 3	0.444369092261707
value 4	0.468326113906509
value 5	0.479044304812892
value 6	0.766654720925613

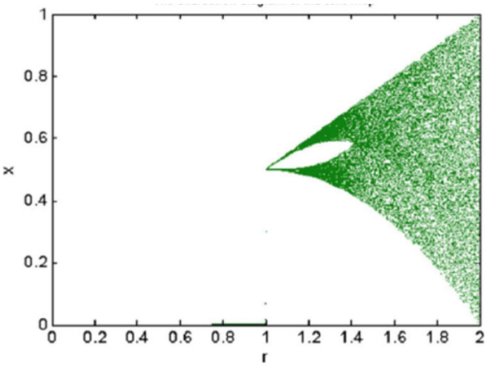

FIGURE 5. Bifurcation diagram of tent map.

the results using the proposed method in the same computer. In other words, compared to methods based on optimization algorithms in terms of performance / user domain knowledge balance, the proposed method offers significant advantages for performance criteria. It is planned to publish various probable initial population sets in the future in order to eliminate possible problems related to user domain knowledge.

The proposed method can be used not only for the logistics map but also for other chaotic maps to obtain initial conditions that will meet the statistical requirements. For example, various chaotic maps that can be used in random number generators are listed in Ref. [35]. Tent map, which is one of these maps with successful randomness values, has been considered as the other analysis study. The mathematical model of the tent map is given in Eq. (3). The bifurcation diagram and Lyapunov exponentials are given in Figure 5 and Figure 6, respectively.

$$x_{n+1} = x_n < 0.5 \; ? \; r^* x_n : r^*(1\text{-}x_n) \tag{3}$$

One of the important reasons for giving Lyapunov exponentials for chaotic maps in Figure 3 and Figure 6 in the study is to explain the selection criteria of control parameters. Lyapunov exponentials are a quantitative indicator of the chaotic behavior of the system. The positive Lyapunov exponential indicates chaotic behavior. Therefore, it is thought that there is a linear relationship between the value of Lyapunov exponents and the disorder of the system (in other words, the quality of the entropy source). Therefore, the control parameter value r = 4 has been chosen for the logistics map.

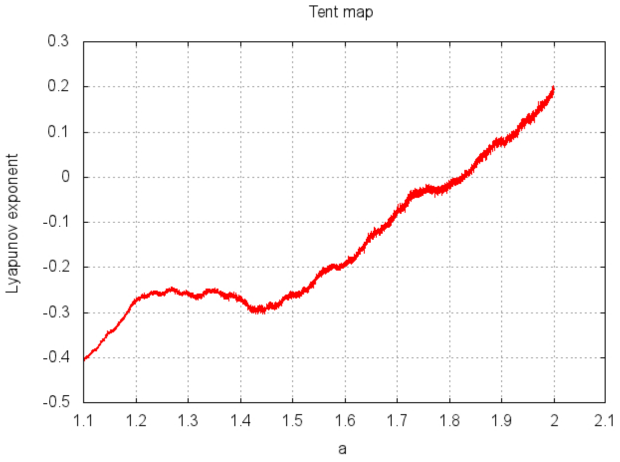

FIGURE 6. Lyapunov exponent diagram of logistic map.

Similarly, the control parameter value r = 1.999 has been chosen for the tent map. Because for these values, the largest Lyapunov exponential values have been obtained.

The obtained initial conditions for tent map using proposed architecture are given in Table 2.

TABLE 2. The obtained initial conditions for tent map.

Initial Conditions	value
value 1	0,1
value 2	0,218815638587692
value 3	0,244926616508738
value 4	0,357025717400358
value 5	0,654444539768341
value 6	0,710352575060545

In information security applications, if the outputs of the generator are used as secret keys, it is thought that determining dynamical the control parameter value with the help of the proposed algorithm instead of choosing a constant is another alternative. In this case, by obtaining a larger key space, a more robust structure can be obtained against brute force attacks. Due to the priority of the performance criterion, this option has not been tried in the study. However, it is planned to investigate these alternatives in future studies.

IV. ANALYSIS RESULTS

Statistical randomness is a basic feature that must be provided for many applications. Therefore, many studies have been carried out to evaluate the statistical properties of the generator. Approaches known as hypothesis tests are often used to check statistical properties. There are many comprehensive test packages in the literature. Among these test packages, the NIST SP 800-22 test package is accepted by many researchers as a standard test tool. NIST SP 800-22 test

TABLE 3. NIST test results for random number sequences which has been generated using initial conditions in the Table 1.

NIST Test Name	Random Sequence 1	Random Sequence 2	Random Sequence 3	Random Sequence 4	Random Sequence 5	Random Sequence 6
Monobit test	P=0.79641	P=0.94579	P=0.68034	P=0.91082	P=0.12552	P=0.82431
Frequency within block test	P=0.7009	P=0.63344	P=0.79594	P=0.31246	P=0.39274	P=0.38561
Runs test	P=0.74286	P=0.75504	P=0.94088	P=0.28824	P=0.51547	P=0.75964
Longest run ones in a block test	P=0.011128	P=0.19989	P=0.48956	P=0.46721	P=0.22471	P=0.37348
Binary matrix rank test	P=1	P=1	P=1	P=1	P=1	P=1
Dft test	P=0.80431	P=0.17442	P=0.08449	P=0.78309	P=0.8688	P=0.33069
Non overlapping template matc.	P=0.46496	P=0.18217	P=0.68789	P=0.83993	P=0.64205	P=0.57506
Overlapping template matching	P=0.5839	P=0.5839	P=0.5839	P=0.5839	P=0.5839	P=0.5839
Maurers universal test	P=0.56922	P=0.56656	P=0.57023	P=0.57004	P=0.56848	P=0.56932
Linear complexity test	P=1	P=1	P=1	P=1	P=1	P=1
Serial test	P=0.91661	P=0.95029	P=0.91625	P=0.56421	P=0.25071	P=0.93046
Approximate entropy test	P=0.88844	P=0.6324	P=0.93674	P=0.56781	P=0.54323	P=0.59561
Cumulative sums test	P=1	P=1	P=1	P=1	P=1	P=1
Random excursion test	P=0.83024	P=0.46499	P=0.97178	P=0.41911	P=0.62029	P=0.6771
Random excursion variant test	P=0.45337	P=0.90175	P=0.51685	P=0.43927	P=0.246	P=0.67157

TABLE 4. NIST test results for random number sequences which has been generated using initial conditions in the Table 1I.

NIST Test Name	Random Sequence 1	Random Sequence 2	Random Sequence 3	Random Sequence 4	Random Sequence 5	Random Sequence 6
Monobit test	P=0,65849	P=0,38321	P=0,04056	P=0,1875	P=0,063454	P=0,18885
Frequency within block test	P=0,85814	P=0,60704	P=0,34744	P=0,64935	P=0,06215	P=0,77268
Runs test	P=0,33495	P=0,32671	P=0,33394	P=0,21414	P=0,92308	P=0,98702
Longest run ones in a block test	P=0,1643	P=0,74693	P=0,46069	P=0,8478	P=0,2739	P=0,94131
Binary matrix rank test	P=1	P=1	P=1	P=1	P=1	P=1
Dft test	P=0,13712	P=1	P=0,067828	P=0,19889	P=0,76902	P=0,25135
Non overlapping template matc.	P=0,12951	P=0,024655	P=0,047931	P=0,27742	P=0,01284	P=0,86711
Overlapping template matching	P=0,5839	P=0,5839	P=0,5839	P=0,5839	P=0,5839	P=0,5839
Maurers universal test	P=0,56938	P=0,57164	P=0,56752	P=0,56799	P=0,5687	P=0,56951
Linear complexity test	P=1	P=1	P=1	P=1	P=1	P=1
Serial test	P=0,452465	P=0,375045	P=0,207262	P=0,203515	P=0,549045	P=0,70286
Approximate entropy test	P=0,057646	P=0,25317	P=0,047028	P=0,64612	P=0,22019	P=0,87009
Cumulative sums test	P=1	P=1	P=1	P=1	P=1	P=1
Random excursion test	P=0,448163	P=0,700375	P=0,452814	P=0,221548	P=0,256564	P=0,400935
Random excursion variant test	P=0,462197	P=0,745527	P=0,438346	P=0,55696	0,297296667	P=0,452156

package contains 15 different tests. Details of these tests can be accessed from Ref. [33].

In this study, the logistic map and tent map have been chosen as the chaotic map for the method detailed in Figure 1. Two random number sequence with a length of 1,000,000 have been generated for six different initial conditions using the proposed model and $r = 4$ (logistic map) and $r = 1.99$ (tent map) control parameter value that would be most suitable for statistical randomness. Two random number sequence of 1,000,000 lengths each have been generated for six different initial conditions (In total, 12 different data sets have been obtained). The NIST SP 800-22 test results of these sequences are given in Table 3 and Table 4, respectively.

The NIST SP 800-22 test suite [33] is one of the most successful statistically accepted test tools. But it is a hypothesis test. "Hypothesis testing is the use of statistics to determine the probability that a given hypothesis is true. The usual process of hypothesis testing consists of four steps.

i. Formulate the null hypothesis H_0 (commonly, that the observations are the result of pure chance) and the alternative hypothesis H_a (commonly, that the observations show a real effect combined with a component of chance variation).
ii. Identify a test statistic that can be used to assess the truth of the null hypothesis.
iii. Compute the P-value, which is the probability that a test statistic at least as significant as the one observed would be obtained assuming that the null hypothesis were true. The smaller the P-value, the stronger the evidence against the null hypothesis.
iv. Compare the p-value to an acceptable significance value alpha (sometimes called an alpha value). If p<=alpha, that the observed effect is statistically

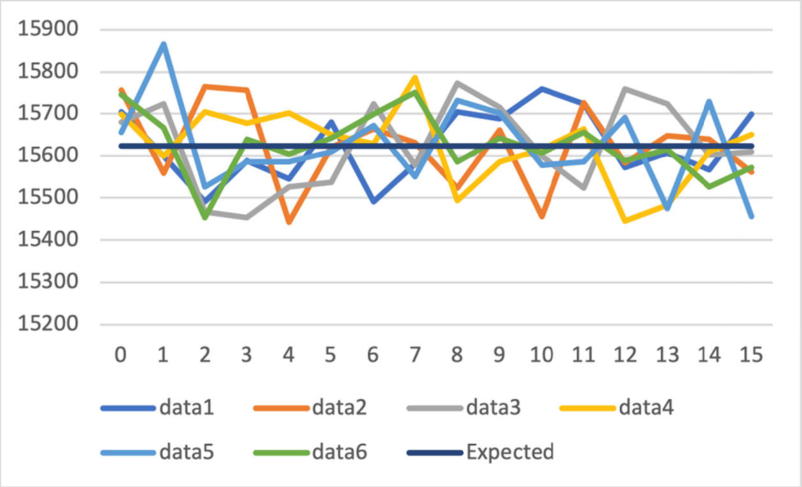

FIGURE 7. Distribution of generated random members using logistic map.

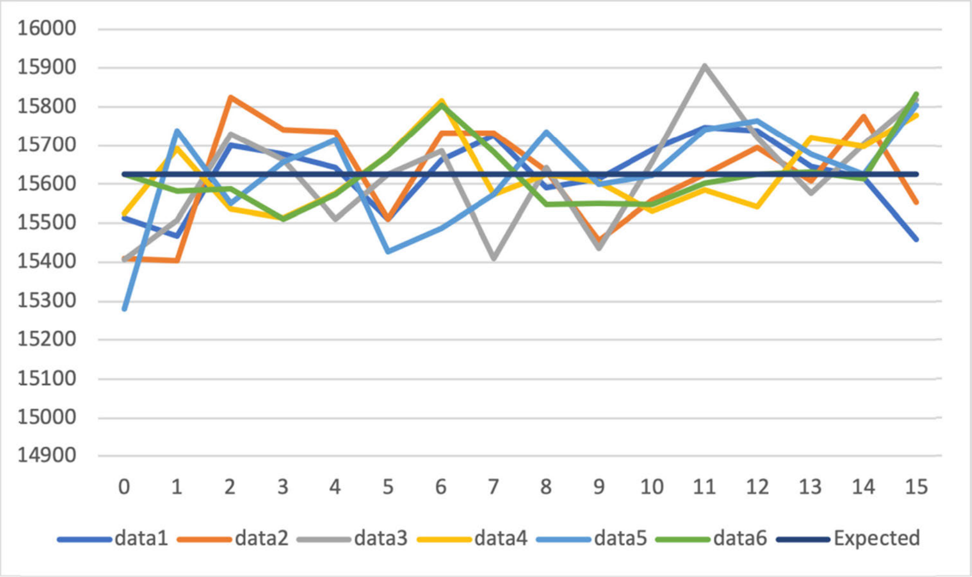

FIGURE 8. Distribution of generated random members using tent map.

> significant, the null hypothesis is ruled out, and the alternative hypothesis is valid.'' [36], [37]

As stated above, p-values must be smaller than the determined alpha values for the test to be successful. P-values given in Table 3 and Table 4 are below the alpha values determined in NIST SP 800-22 test suite. However, these results do not fully prove that the generated random numbers are statistically strong. With a newly designed statistical test, the generator has the potential to fail this statistical test successfully. Therefore, 1,000,000 bit value is divided into 4-bit blocks and converted to 250,000 decimal value between 0-15 to show the statistical success of the generator. Figure 7 and Figure 8 show the distribution of values converted to decimal values between 0-15 for six different initial conditions in Table 1 and Table 2. In addition, Table 5 and Table 6 can be examined to analyze how many of each number are produced.

There are sixteen different options as the value ranges are from 0-15. Therefore, ideally, the number of each decimal value is expected to be 250,000/16=15,625. It is clearly observed from Figure 7 and Figure 8 that the distributions of generated random numbers for the six different initial conditions in Table 1 and Table 2 have a uniform distribution. After converting the generated bit sequences to decimal values, another statistical test has been applied. In this test approach known as chi-square test, it is possible to make a quantitative evaluation using the confidence intervals determined. Since the generated bit sequence is converted to

TABLE 5. Distribution of decimal values for generated using logistic map.

Data	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
data1	15704	15599	15491	15588	15544	15680	15492	15579	15705	15690	15760	15723	15571	15607	15567	15700
data2	15757	15559	15766	15757	15441	15621	15665	15633	15523	15663	15456	15728	15583	15649	15639	15560
data3	15682	15723	15466	15454	15527	15536	15725	15578	15774	15717	15600	15523	15759	15723	15602	15611
data4	15700	15599	15706	15677	15703	15652	15630	15786	15493	15586	15615	15664	15445	15484	15609	15651
data5	15655	15865	15527	15586	15586	15609	15673	15550	15731	15703	15577	15587	15691	15474	15730	15456
data6	15747	15667	15452	15640	15604	15642	15700	15751	15586	15644	15608	15657	15589	15616	15526	15571
Expected	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625

TABLE 6. Distribution of decimal values for generated using tent map.

Dataset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
data1	15514	15468	15701	15678	15642	15510	15662	15726	15590	15615	15689	15746	15739	15645	15617	15458
data2	15409	15404	15825	15740	15734	15512	15732	15733	15634	15457	15559	15626	15696	15610	15776	15553
data3	15407	15509	15731	15664	15510	15625	15685	15409	15643	15437	15657	15904	15720	15577	15703	15819
data4	15524	15692	15538	15513	15578	15674	15817	15575	15625	15606	15531	15587	15541	15722	15698	15779
data5	15280	15737	15551	15658	15715	15428	15487	15575	15734	15601	15624	15740	15764	15677	15625	15804
data6	15626	15582	15588	15510	15575	15674	15805	15683	15548	15552	15547	15604	15625	15632	15615	15834
Expected	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625	15625

TABLE 7. The confidence values for degree of freedom 16.

DF	0.995	0.975	0.20	0.10	0.05	0.025	0,01	0,005	0,002	0,001
value	5.142	6.908	20.465	23.542	26.296	28.845	32.000	34.267	37.146	39.252

TABLE 8. Chi-square test results.

Dataset	Logistic Map	Tent Map
dataset 1	6.804224	18.325504
dataset 2	8.83968	19.6352
dataset 3	10.693632	16.793472
dataset 4	7.814656	7.598208
dataset 5	10.697088	16.793472
dataset 6	5.524608	8.4512

16 different decimal values, the degree of freedom of the test is 16. All confidence values for degree of freedom 16 are given in Table 7. The calculated chi-square values for dataset produced in Table 5 and Table 6 are given in Table 8. When the calculated chi-square values are analyzed, it shows that all datasets are acceptable for 0.20 confidence value. However, it can be stated that dataset6 is statistically more suitable among these datasets.

It should be noted that all the analyzes given in this section are statistical hypothesis tests. In other words, even a generator that has successfully passed all the tests may not be able to provide a new test. Therefore, it cannot be used directly in certain cryptographic applications. The reason for drawing attention to this kind of disadvantage is that the main aim in the studies on chaos based random bit generators is to realize practical designs that can be used in cryptographic applications. In the following section, the outputs of the proposed method are used in the design of a cryptographic component that has a critical importance in information security applications. Thus, a practical application of the proposed method is also shown.

V. A PRACTICAL APPLICATION OF GENERATED RANDOM BIT SEQUENCES IN CRYPTOGRAPHY

The determined initial conditions using the proposed method in the study provide both NIST SP 800-22 and chi-square tests. The design problem in chaos-based random number generators is that there are an infinite number of possibilities to select initial conditions. This design problem is inherently an NP problem. Optimization algorithms can be used to find an approximate solution to this problem [34]. However, optimization algorithms may have a disadvantage in practical applications due to computational difficulty. Since performance is also a critical evaluation criterion in cryptology applications, a method that is more convenient than optimization algorithms has been proposed in terms of performance. In order to analyze the success of this method in practical applications, the design of the substitution box (s-box) structures has been investigated using the obtained random bit sequences. S-box structures are a

TABLE 9. S-box structure generated form logistic map.

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

nonlinear component in block cipher systems, they directly affect the encryption requirements such as confusion. One of the most important reasons affecting the transition from DES (Data Encryption Standard) algorithm to AES (Advanced Encryption Standard) algorithm is differential attacks on s-box structures. Therefore, researchers focus on alternative s-box designs approaches. Particularly with the popularity of practical cryptanalysis techniques such as side channel attacks, interest in s-box design techniques based on random selection techniques has increased [38].

In this section, a s-box design approach is proposed based on generated random number sequences based on chaotic map. The design logic of the proposed method is detailed in the flowchart in Figure 9. Two different s-box structures generated for a random bit sequence obtained using two different datasets produced by using logistic map and the tent map are given in Table 9 and Table 10, respectively. There are five basic criteria to evaluate the success of the produced s-box structures. Ref. [39] can be examined for both detailed information about these criteria and an analysis program that can be used free of charge. Analysis results regarding these criteria are given in Table 11. Table 11 presents performance analysis of both the generated s-box structures and the various designs proposed recently. Therefore, the opportunity to evaluate the success of the proposed method has been provided.

It is necessary to evaluate the references given in Table 11 in two different categories. Because Ref. [40]–[45] is based on mathematical transformations. It can be observed that these designs are closed to ideal values for both the nonlinearity criterion and the XOR value. Ideal values refer to structures with analysis results equivalent to the AES s-box structure. The nonlinearity value is 112 and the XOR value is 4 for the AES s-box structure. However, it has been observed that these studies only focused on various criteria. For example, it has been observed that while the desired value has been obtained for the nonlinear value, the condition for the XOR value has not been met in Ref. [40]–[42]. In the approaches suggested in Ref. [43]–[45], the design criteria have been reached. It has also been shown in different studies that a similar approach can be achieved by optimizing the results [46], [47]. Although there is a possibility to use these design approaches to improve s-box criteria; the performance of s-box structures to be generated from random bit sequences have been analyzed. Therefore, it is considered to be more fair to compare the produced s-box structures with the other references presented

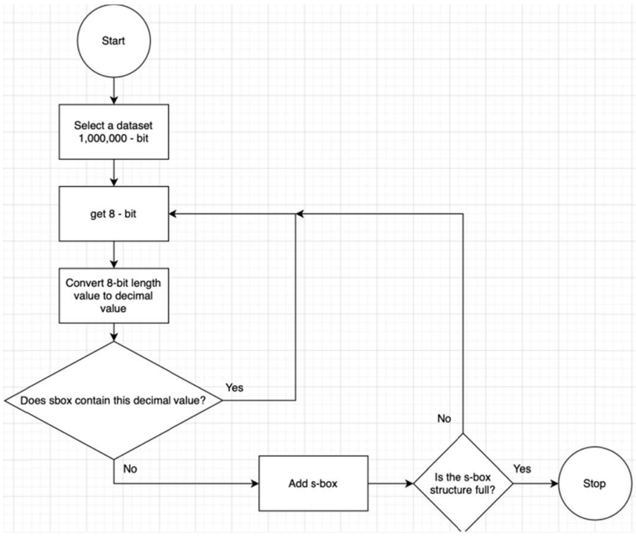

FIGURE 9. General design approach for chaos-based entropy pool [33].

TABLE 10. S-box structure generated form tent map.

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

TABLE 11. Performance comparison for s-box structures.

S-box	Nonlinearity			Bit Independence Criterion		Strict Avalanche Criterion			Maximum I/O XOR
	min	max	avg	Non.	SAC	avg	max	min	
Ref. [40]	106	108	106.5	103.5	0.5033	0.4990	0.5781	0.4063	10
Ref. [41]	110	112	111.25	111.5	0.4950	0.5068	0.5781	0.4063	10
Ref. [42]	110	112	111.25	102.5	0.5034	0.5007	-	-	10
Ref. [43]	112	112	112	112	0.4890	0.504	-	-	4
Ref. [44]	112	112	112	112	0.5013	0.5053	0.5625	0.4375	4
Ref. [45]	112	112	112	112	-	0.4951	-	-	4
Ref. [46]	102	106	105	103.6	0.5004	0.5046	0.6093	0.4750	10
Ref. [47]	106	112	109.5	106.8	-	0.5068	-	-	8
Ref. [48]	104	110	107.5	103.5	-	0.4980	-	-	10
Ref. [49]	-	-	106	-	-	-	0.5781	0.4219	10
Ref. [50]	106	110	108	104.2	0.4961	0.4990	0.5781	0.4063	10
Ref. [51]	99	106	103.3	103.6	0.5037	0.5058	0.625	0.4062	12
Ref. [52]	88	163	-	102	0.4990	0.4950	-	-	15
Ref. [53]	-	-	102	-	-	-	-	-	8
Ref. [54]	106	110	108.5	104	0.4971	0.5017	0.5938	0.4062	10
Ref. [55]	104	110	106	103.5	0.4977	0.5012	0.6406	0.4062	10
Ref. [56]	102	110	105.5	104.3	0.4988	0.5010	0.6094	0.4063	12
Ref. [57]	104	106	105	103.4	0.4994	0.5012	0.5938	0.4063	10
Ref. [58]	102	108	104.5	104.6	0.5013	0.498	0.6406	0.4219	12
Ref. [59]	102	108	105.3	104	0.4971	0.5056	0.5781	0.4375	10
Ref. [60]	102	108	105.25	102.6	0.4994	0.5037	0.5625	0.4375	10
Ref. [61]	104	110	106	104.2	0.5014	0.5197	0.625	0.4375	10
Table IX	98	108	105.25	103,86	0.4986	0.5073	0.6094	0.4062	10
Table X	102	108	105.75	102,36	0.4972	0.4062	0.5938	0.5027	10

in the Table 11. Another point to note is that the s-box structures presented in Table 9 and Table 10 are the first s-box structures produced from bit sequences obtained from chaotic maps. Maybe better or worse s-box structures can be obtained. However, such a comprehensive analysis has not been carried out in order to make a fair evaluation of the study. From the analysis results; It has been observed that the produced s-box structures have values close to the designs in the literature.

Although the proposed s-box structures have average performance criteria, their biggest advantage is that they will be more resistant to side channel attacks than mathematical designs [38]. In addition to these advantages, it is thought that a dynamic s-box structure can be generated by using different initial conditions. For example, it can be used instead of the s-box structures in Ref. [61], as well as in successful image encoding algorithms in the literature [62], [63].

Another practical application of the proposed method is that the initial conditions and control parameters of chaotic systems can be used as the secret key of the encryption algorithm in these designs. A strong feature in chaos-based random bit generators is the guarantee of a large key space. For example, the initial condition and control parameter of the Logistic map are expressed in 52 bits each. So even the key of a simple design will be $2*52 = 104$ bits. An attack scenario will be addressed because it is greater than the 80-bit limit value accepted for attacks known as brute force attack.

VI. CONCLUSION

The initial conditions determined using the proposed method in the study provide both The NIST SP 800-22 and chi-square tests. The design problem in chaos-based random number generators is that there are an infinite number of possibilities to select initial conditions. This design problem is inherently an NP problem. Optimization algorithms can be used to find an approximate solution to this problem. optimization algorithms have several computational difficulties. In this study, a method that attempts to solve the success achieved with optimization algorithms using a simpler method is proposed. The problem is determining the most suitable initial conditions of chaotic systems that will provide statistical randomness in the best way is analyzed. A model similar to artificial neural network architecture has been proposed to solve this problem. The proposed approach has been tried to overcome the computational difficulty of the problem. Six different initial conditions of the logistic map and tent map have been calculated using the proposed method. Random number sequences have been generated using the determined initial conditions. The statistical properties of the generated random number sequences have been checked with The NIST SP 800-22 test suite. The analysis results showed that the determined initial conditions successfully provided all randomness tests.

The obtained results in this study are important as they have verified the study previously performed using optimization algorithms. In previous study [34], using the six optimization algorithms for four different chaotic systems, the most appropriate initial conditions and control parameters have been determined. In this study, it is aimed to determine only the most suitable initial conditions based on the assumption that the best statistical properties can be reached for the value of control parameter 4. In this way, the computational complexity of the method is better than the previous method. However, similar studies should be carried out in different chaotic systems in future studies. Another study planned in the future is to investigate both the initial conditions and the selection of control parameters together, as in the previous study.

ACKNOWLEDGMENT

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.

REFERENCES

[1] S. Strogatz, *Nonlinear Dynamics And Chaos: With Applications To Physics, Biology, Chemistry, And Engineering* (Studies in Nonlinearity). Boulder, CO, USA: Westview, 2015.

[2] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, Mar. 1963.

[3] F. Özkaynak, "Cryptographically secure random number generator with chaotic additional input," *Nonlinear Dyn*, vol. 78, pp. 2015–2020, 2014, doi: 10.1007/s11071-014-1591-y.

[4] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity," *Symmetry*, vol. 11, no. 2, p. 140, Jan. 2019.

[5] M. Alawida, A. Samsudin, J. S. Teh, and W. H. Alshoura, "Digital cosine chaotic map for cryptographic applications," *IEEE Access*, vol. 7, pp. 150609–150622, 2019, doi: 10.1109/ACCESS.2019.2947561.

[6] S. E. El-Khamy, N. O. Korany, and A. G. Mohamed, "A new fuzzy-DNA image encryption and steganography technique," *IEEE Access*, vol. 8, pp. 148935–148951, 2020, doi: 10.1109/ACCESS.2020.3015687.

[7] V. Schindler, "Random number generators for cryptographic applications," in *Cryptographic Engineering* (Signals and Communication Theory), C. K. Koc, Ed. Berlin, Germany: Springer, 2009.

[8] E. Avaroğlu, T. Tuncer, A. B. Özer, B. Ergen, and M. Türk, "A novel chaos-based post-processing for TRNG," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 189–199, Jul. 2015, doi: 10.1007/s11071-015-1981-9.

[9] M. Stipčević and Ç. K. Koç, "True random number generators," in *Open Problems in Mathematics and Computational Science*, K. Koç, Ed. Cham, Switzerland: Springer, 2014.

[10] V. B. Suresh and W. P. Burleson, "Entropy extraction in metastability-based TRNG," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*. Anaheim, CA, USA: IEEE, Jun. 2010, pp. 135–140.

[11] M. Dichtl, "Bad and good ways of post-processing biased physical random numbers," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 4593, A. Biryukov, Ed. Berlin, Germany: Springer, 2007, pp. 137–152.

[12] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007.

[13] A. M. Garipcan and E. Erdem, "A TRNG using chaotic entropy pool as a post-processing technique: Analysis, design and FPGA implementation," *Anal. Integr. Circuits Signal Process.*, vol. 103, no. 3, pp. 391–410, Jun. 2020, doi: 10.1007/s10470-020-01605-0.

[14] E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via zigbee channels," *Chaos, Solitons Fractals*, vol. 133, Apr. 2020, Art. no. 109646, doi: 10.1016/j.chaos.2020.109646.

[15] E. Avaroğlu and T. Tuncer, "A novel S-box-based postprocessing method for true random number generation," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 28, no. 1, pp. 288–301, Jan. 2020, doi: 10.3906/elk-1906-194.

[16] O. Guillén-Fernández, A. Meléndez-Cano, E. Tlelo-Cuautle, J. C. Núñez-Pérez, and J. de Jesus Rangel-Magdaleno, "On the synchronization techniques of chaotic oscillators and their FPGA-based implementation for secure image transmission," *PLoS ONE*, vol. 14, no. 2, pp. 1–34, 2019, doi: 10.1371/journal.pone.0209618.

[17] E. Rodríguez-Orozco, E. García-Guerrero, E. Inzunza-Gonzalez, O. López-Bonilla, A. Flores-Vergara, J. Cárdenas-Valdez, and E. Tlelo-Cuautle, "FPGA-based chaotic cryptosystem by using voice recognition as access key," *Electronics*, vol. 7, no. 12, p. 414, Dec. 2018, doi: 10.3390/electronics7120414.

[18] A. Flores-Vergara, E. Inzunza-González, E. García-Guerrero, O. López-Bonilla, E. Rodríguez-Orozco, J. Hernández-Ontiveros, J. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Implementing a chaotic cryptosystem by performing parallel computing on embedded systems with multiprocessors," *Entropy*, vol. 21, no. 3, p. 268, Mar. 2019, doi: 10.3390/e21030268.

[19] L. Kocarev and S. Lian, *Chaos Based Cryptography Theory Algorithms and Applications*. Berlin, Germany: Springer-Verlag, 2011.

[20] L. Ding, C. Liu, Y. Zhang, and Q. Ding, ''A new lightweight stream cipher based on chaos,'' *Symmetry*, vol. 11, no. 7, p. 853, Jul. 2019.

[21] K. Demir and S. Ergün, ''An analysis of deterministic chaos as an entropy source for random number generators,'' *Entropy*, vol. 20, no. 12, p. 957, Dec. 2018.

[22] D. Lambić and M. Nikolić, ''Pseudo-random number generator based on discrete-space chaotic map,'' *Nonlinear Dyn.*, vol. 90, no. 1, pp. 223–232, Oct. 2017, doi: 10.1007/s11071-017-3656-1.

[23] F. Ozkaynak, ''A novel random number generator based on fractional order chaotic Chua system,'' *Elektronika ir Elektrotechnika*, vol. 26, no. 1, pp. 52–57, Feb. 2020, doi: 10.5755/j01.eie.26.1.25310.

[24] J. V. C. Evangelista, J. A. P. Artiles, D. P. B. Chaves, and C. Pimentel, ''Emitter-coupled pair chaotic generator circuit,'' *AEU-Int. J. Electron. Commun.*, vol. 77, pp. 112–117, Jul. 2017, doi: 10.1016/j.aeue.2017.04.029.

[25] S. Vaidyanathan, A. Akgul, S. Kaçar, and U. Çavuşoğlu, ''A new 4-D chaotic hyperjerk system, its synchronization, circuit design and applications in RNG, image encryption and chaos-based steganography,'' *Eur. Phys. J. Plus*, vol. 133, no. 2, p. 46, Feb. 2018.

[26] M. Bakiri, C. Guyeux, J.-F. Couchot, and A. K. Oudjida, ''Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses,'' *Comput. Sci. Rev.*, vol. 27, pp. 135–153, Feb. 2018, doi: 10.1016/j.cosrev.2018.01.002.

[27] S. Kaçar, ''Analog circuit and microcontroller based RNG application of a new easy realizable 4D chaotic system,'' *Optik*, vol. 127, no. 20, pp. 9551–9561, Oct. 2016, doi: 10.1016/j.ijleo.2016.07.044.

[28] B. Karakaya, A. Gülten, and M. Frasca, ''A true random bit generator based on a memristive chaotic circuit: Analysis, design and FPGA implementation,'' *Chaos, Solitons Fractals*, vol. 119, pp. 143–149, Feb. 2019, doi: 10.1016/j.chaos.2018.12.021.

[29] Ü. Çavuşoğlu, A. Akgül, A. Zengin, and I. Pehlivan, ''The design and implementation of hybrid RSA algorithm using a novel chaos based RNG,'' *Chaos, Solitons Fractals*, vol. 104, pp. 655–667, Nov. 2017, doi: 10.1016/j.chaos.2017.09.025.

[30] P. F. Verhulst, ''Resherches mathematiques sur la loi d'accroissement de la population,'' *Nouveaux memoires de l'academie royale des sciences*, vol. 18, no. 1, pp. 1–41, 1845.

[31] R. M. May, ''Simple mathematical models with very complicated dynamics,'' *Nature*, vol. 261, no. 5560, pp. 459–467, Jun. 1976.

[32] J. Sprott, *Elegant Chaos: Algebraically Simple Chaotic Flows*. Singapore: World Scientific, 2010.

[33] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, ''A statistical test suite for random and pseudorandom number generators for cryptographic applications,'' NIST Special Publication, Gaithersburg, MD, USA, Tech. Rep. 800-22rev1a, 2010.

[34] 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.

[35] L. G. de la Fraga, E. Torres-Pérez, E. Tlelo-Cuautle, and C. Mancillas-López, ''Hardware implementation of pseudo-random number generators based on chaotic maps,'' *Nonlinear Dyn.*, vol. 90, no. 3, pp. 1661–1670, Nov. 2017, doi: 10.1007/s11071-017-3755-z.

[36] *Hypothesis Testing*. Accessed: Dec. 12, 2020. [Online]. Available: https://mathworld.wolfram.com/HypothesisTesting.html

[37] M. A. Martin, ''Bootstrap hypothesis testing for some common statistical problems: A critical evaluation of size and power properties,'' *Comput. Statist. Data Anal.*, vol. 51, no. 12, pp. 6321–6342, Aug. 2007.

[38] M. S. Acikkapi, F. Ozkaynak, and A. B. Ozer, ''Side-channel analysis of chaos-based substitution box structures,'' *IEEE Access*, vol. 7, pp. 79030–79043, 2019, doi: 10.1109/ACCESS.2019.2921708.

[39] F. Özkaynak, ''An analysis and generation toolbox for chaotic substitution boxes: A case study based on chaotic labyrinth rene thomas system,'' *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 44, no. 1, pp. 89–98, Mar. 2020, doi: 10.1007/s40998-019-00230-6.

[40] W. Gao, B. Idrees, S. Zafar, and T. Rashid, ''Construction of nonlinear component of block cipher by action of modular group PSL(2,Z) on projective line PL(GF(2^8)),'' *IEEE Access*, vol. 8, pp. 136736–136749, 2020, doi: 10.1109/ACCESS.2020.3010615.

[41] A. Razaq, A. Ullah, H. Alolaiyan, and A. Yousaf, ''A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers,'' *Wireless Pers. Commun.*, Oct. 2020, doi: 10.1007/s11277-020-07841-x.

[42] M. Ahmad and E. Al-Solami, ''Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme,'' *Entropy*, vol. 22, no. 7, p. 717, Jun. 2020.

[43] M. S. Mahmood Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-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.

[44] N. Siddiqui, H. Khalid, F. Murtaza, M. Ehatisham-Ul-Haq, and M. A. Azam, ''A novel algebraic technique for design of computational substitution-boxes using action of matrices on Galois field,'' *IEEE Access*, vol. 8, pp. 197630–197643, 2020, doi: 10.1109/ACCESS.2020.3034832.

[45] N. Siddiqui, F. Yousaf, F. Murtaza, M. Ehatisham-Ul-Haq, M. U. Ashraf, A. M. Alghamdi, and A. S. Alfakeeh, ''A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field,'' *PLoS ONE*, vol. 15, no. 11, Nov. 2020, Art. no. e0241890, doi: 10.1371/journal.pone.0241890.

[46] F. Artuğer and F. Özkaynak, ''A novel method for performance improvement of chaos-based substitution boxes,'' *Symmetry*, vol. 12, no. 4, p. 571, Apr. 2020.

[47] 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.

[48] A. H. Zahid, E. Al-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.

[49] 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, doi: 10.1109/ACCESS.2020.3032403.

[50] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad, M. S. Hossain, and A. M. Abbas, ''Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps,'' *IEEE Access*, vol. 8, pp. 160433–160449, 2020, doi: 10.1109/ACCESS.2020.3020746.

[51] N. Hematpour and S. Ahadpour, ''Execution examination of chaotic S-box dependent on improved PSO algorithm,'' *Neural Comput. Appl.*, Aug. 2020, doi: 10.1007/s00521-020-05304-9.

[52] O. Sengel, M. A. Aydin, and A. Sertbas, ''An efficient generation and security analysis of substitution box using fingerprint patterns,'' *IEEE Access*, vol. 8, pp. 160158–160176, 2020, doi: 10.1109/ACCESS.2020.3021055.

[53] A. Freyre-Echevarria, I. Martinez-Diaz, C. M. L. Perez, G. Sosa-Gomez, and O. Rojas, ''Evolving nonlinear S-boxes with improved theoretical resilience to power attacks,'' *IEEE Access*, vol. 8, pp. 202728–202737, 2020, doi: 10.1109/ACCESS.2020.3035163.

[54] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, ''A new hyperchaotic system-based design for efficient bijective substitution-boxes,'' *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018, doi: 10.3390/e20070525.

[55] U. Çavuşoğlu, S. Kaçar, A. Zengin, and I. Pehlivan, ''A novel hybrid encryption algorithm based on chaos and S-AES algorithm,'' *Nonlinear Dyn*, vol. 92, pp. 1745–1759, Mar. 2018, doi: 10.1007/s11071-018-4159-4.

[56] A. Belazi and A. A. A. El-Latif, ''A simple yet efficient S-box method based on chaotic sine map,'' *Optik*, vol. 130, pp. 1438–1444, Feb. 2017.

[57] F. Özkaynak, ''From biometric data to cryptographic primitives: A new method for generation of substitution boxes,'' in *Proc. ACM Int. Conf. Biomed. Eng. Bioinf.*, Bangkok, Thailand, Sep. 2017, pp. 27–33, doi: 10.1145/3143344.3143355.

[58] L. Liu, Y. Zhang, and X. Wang, ''A novel method for constructing the S-box based on spatiotemporal chaotic dynamics,'' *Appl. Sci.*, vol. 8, no. 12, p. 2650, Dec. 2018, doi: 10.3390/app8122650.

[59] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, ''Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption,'' *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, 2017.

[60] F. Özkaynak, ''On the effect of chaotic system in performance characteristics of chaos based S-box designs,'' *Phys. A, Stat. Mech. Appl.*, vol. 550, Jul. 2020, Art. no. 124072, doi: 10.1016/j.physa.2019.124072.

[61] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. Vo Hoang, and X. Nguyen, ''A chaotic system with infinite equilibria and its S-box constructing application,'' *Appl. Sci.*, vol. 8, no. 11, p. 2132, Nov. 2018, doi: 10.3390/app8112132.

[62] Z. M. Z. Muhammad and F. Ozkaynak, "An image encryption algorithm based on chaotic selection of robust cryptographic primitives," *IEEE Access*, vol. 8, pp. 56581–56589, 2020, doi: 10.1109/ACCESS.2020.2982827.

[63] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020, doi: 10.1109/ACCESS.2020.3020917.

[64] E. Tlelo-Cuautle, V. H. Carbajal-Gomez, P. J. Obeso-Rodelo, J. J. Rangel-Magdaleno, and J. C. Nuñez-Pérez, "FPGA realization of a chaotic communication system applied to image processing," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1879–1892, Dec. 2015, doi: 10.1007/s11071-015-2284-x.

MEHMET Ş. AÇIKKAPI was born in Palu, Turkey. He received the bachelor's and master's degrees in computer engineering from Firat University. During his graduate studies, he worked on generation and analysis of one-time password for mobile devices. In the Ph.D. studies, he studies side-channel analysis of chaos-based encryption systems. He is also a Lecturer with the Department of Computer Technologies, Munzur University. He has published his results in various journals and conferences.

FATIH ÖZKAYNAK received the B.Sc. and M.Sc. degrees in computer engineering from Fırat University, Elâzığ, Turkey, in 2005 and 2007, respectively, and the Ph.D. degree in computer engineering from Yildiz Technical University, in 2013.

He is currently an Associate Professor of software engineering with Fırat University. He has coauthored more than 75 refereed scientific journal and conference papers. His works have been cited more than 1000 times. He has taught algorithm and programming, programming language, artificial intelligence, and cryptography courses at Fırat University. He has supervised four M.Sc. and two Ph.D. students toward their graduation project in information security and cryptography area. His research interests include cryptography, information security, and chaotic systems.

Dr. Özkaynak serves as a Reviewer for scientific journals, including *Cryptography and Communications—Discrete Structures*, *Boolean Functions and Sequences*, *Information Sciences*, the IEEE Transactions on Very Large Scale Integration Systems, *IET Information Security*, *Security and Communication Networks*, *Computers & Electrical Engineering*, *Applied Soft Computing*, *Physics Letter A*, and *Applied Mathematical Modelling*.