Turkish Journal of Science & Technology
18(2), 387-395, 2023

Research Paper
https://doi.org/10.55525/tjst.1287092

An Analysis Tool for Cryptographic Designs Based on Chaotic Systems

Yılmaz AYDIN[1*], Fatih ÖZKAYNAK[2]

[1*] Department of Software Engineering, Faculty of Engineering, Firat University, Elazig, Turkey
[2] Department of Software Engineering, Faculty of Technology, Firat University, Elazig, Turkey
[1*] y.aydin@firat.edu.tr , [2] ozkaynak@firat.edu.tr

(Geliş/Received: 24/04/2023; Kabul/Accepted: 18/08/2023)

Abstract: Chaos-based cryptography research is one of the application areas for chaotic systems. Numerous design studies have been put up that take use of the connection between chaos and cryptography. This study has demonstrated how to exploit this relationship to decrypt cryptography designs. It has been looked at if chaos analysis techniques may be used to analyze cryptography protocols. The effectiveness of random number generators has been evaluated using Lyapunov exponents, a chaos analysis technique. The findings of the investigation demonstrated that Lyapunov exponents can be utilized as a standard in assessing random number generators. The paper highlights the issues with the NIST test suite, a popular method of analysis for assessing the statistical characteristics of random number generators. These issues have been seen to not exist with the new test tool that has been suggested. These findings demonstrate that the suggested strategy can be successfully applied in a variety of future applications.

Key words: Chaos, Cryptography, Lyapunov Exponents, Random Numbers.

Kaotik Sistemler Tabanlı Kriptografik Tasarımlar için Bir Analiz Aracı

Öz: Kaos tabanlı kriptografi araştırmaları, kaotik sistemlerin uygulama alanlarından biridir. Kaos ve kriptografi arasındaki bağlantıdan yararlanan çok sayıda tasarım çalışması yapılmıştır. Bu çalışma, kriptografi tasarımlarının şifresini çözmek için bu ilişkinin nasıl kullanılacağını göstermiştir. Kriptografi protokollerini analiz etmek için kaos analiz tekniklerinin kullanılıp kullanılamayacağına bakılmıştır. Rastgele sayı üreteçlerinin etkinliği, bir kaos analizi tekniği olan Lyapunov üstelleri kullanılarak değerlendirilmiştir. Araştırmanın bulguları, Lyapunov üstellerinin rasgele sayı üreteçlerini değerlendirmede bir standart olarak kullanılabileceğini göstermiştir. Makale, rasgele sayı üreteçlerinin istatistiksel özelliklerini değerlendirmek için popüler bir analiz yöntemi olan NIST test takımıyla ilgili sorunları vurgulamaktadır. Önerilen yeni test aracı ile bu sorunların olmadığı görülmüştür. Bu bulgular, önerilen stratejinin gelecekteki çeşitli uygulamalarda başarıyla uygulanabileceğini göstermektedir.

Anahtar kelimeler: Kaos, kriptografi, Lyapunov Üsleri, Rastgele sayılar

1. Introduction

The main purpose of science and engineering studies is to understand real world systems and to use these results for the benefit of mankind. During these studies, chaos theory became increasingly important. Because this phenomenon is needed to understand the logic of real world events. Therefore, chaos theory has started to find its place in many applications [1]. One of the most common practical applications is the design of chaos based encryption systems [2]. In the simplest expression, chaos theory is defined as the randomness of a deterministic system. In other words, despite the fact that real world events are mathematical models, they contain an unpredictable randomness. This exciting relationship is the fundamental phenomenon desired in the cryptographic system design process [3]. A cryptographic protocol is an algorithm. However, this algorithm should provide two basic requirements, called confusion and diffusion. Chaos based cryptography studies have become increasingly popular among researchers over the last two decades, since chaotic systems have both a mathematical model and the randomness properties will provide confusion and diffusion requirements [4].
This close relationship between chaos theory and cryptography science has been used in the design process.
In other words, chaotic systems have been used as an entropy source and this entropy source has been transformed into cryptographic primitives such as image encryption schema [2, 5, 6, 7, 8], hash functions [9, 10], s-box designs [11, 12] and key generators with the help of a protocol [13-17]. Again, random numbers and bits have been generated with FPGA using chaos-based maps in studies in the literature [18-20].

* Corresponding author: y.aydin@firat.edu.tr ORCID Number of authors: [1]0000-0001-6057-3693 , [2] 0000-0003-1292-8490

When the common aspects of these cryptographic primitive studies are examined, it is seen that the hypotheses of the researchers are based on the fact that the complexity of the entropy source contributes to the design of the cryptographic primitive. In other words, it is claimed that there is a strong relationship between the complexity of the chaotic system used as an entropy source and the robustness of the cryptographic protocols [2, 3, 4].
This study approaches this theory from a different angle. It has been looked at if chaos analysis techniques may be used to analyze cryptography protocols. The work tries to prove the notion that chaos analysis methods can be used to evaluate the quality of these cryptographic protocols if the complexity of the chaotic system employed in the protocol design contributes positively to it. This notion was tested in this study using cryptographic random number generators.
Random number generators used in cryptography have been evaluated for quality using Lyapunov exponents, a chaos analysis technique. The findings of the investigation demonstrated that Lyapunov exponents can be utilized as a standard in assessing random number generators. These findings supported the putative idea. It has also demonstrated that it might offer a different way to handle issues when testing the statistical characteristics of applications that require short length sequences, particularly cryptographic key generators.
The remainder of the research is structured as follows. In the second section, it was briefly described how to calculate the Lyapunov exponents for a dataset using chaos analysis methods. The design architecture of the chaos-based random number generator is described in the third section. alternative datasets for three alternative initial circumstances and control parameter values of the chaotic system employed in the generator have been obtained, and they are presented in this section. The system exhibits periodic, chaotic, and optimally chaotic behavior for the chosen initial circumstances and control parameters. Results of the randomness test and Lyapunov analyses for various datasets are presented in the fourth section. The link between the results of the two investigations demonstrates that the purported hypothesis is accurate. The final section includes a summary of the findings and recommendations for additional research.

2. Materials & Methods

2.1. Chaos Analysis with Lyapunov Exponents

Since chaotic behavior is an important characteristic, many researchers want to examine the existence of chaos in their systems [21, 22]. In this process, methods such as phase space portrait, power spectrum, Poincare mapping bifurcation diagram have been some of the most common methods used to determine chaotic behavior. However, the common point of these methods is that they are qualitative approaches. In other words, there is a need for an expert to interpret and evaluate the results. The chaos analysis method known as Lyapunov exponents has become more popular than others because it is a quantitative approach [22].
The idea that fixed (invariant) exponents could be used to determine the stability states of the sets of differential equations of nonlinear dynamic systems was first shown by Sonya Kovalevskaya in 1889. Following the introduction of this hypothesis, it was based on theoretical foundations by Alexandr Mikhailovich Lyapunov. In the Lyapunov study, he explained only the basics of his thoughts about the change of trajectories of a dynamic system (as a function of time) with Lyapunov exponents. The reliance of chaotic systems on their initial circumstances and control settings serves as the foundation for chaos analysis utilizing Lyapunov exponents. Chaos analysis can be done by relocating the orbits away from one another or by allowing them to converge in situations where a chaotic system is formed from two very close neighboring beginning conditions. A mathematical technique that gauges this separation between adjacent orbits is the use of Lyapunov exponents. Lyapunov exponentials are likened to eigenvalues used in linear systems [21, 22].
Lyapunov exponents can be calculated for continuous time system, discrete time systems and time series obtained from experimental or simulation results. Sensitivity to the initial conditions of a dynamic system is measured by Lyapunov exponents. Firstly, two trajectories have been determined with very close initial conditions on an attractor. If the attractor is showing chaotic behavior, the orbits are divided on an exponential rate, characterized by the largest Lyapunov exponent. The detection of a positive Lyapunov exponential is sufficient for the existence of chaos and indicates instability in a particular direction.
The TISEAN 3.0.0 package will be used for the calculation of Lyapunov exponents [23]. There are two different algorithms to make the calculations using the program. These algorithms have been developed by Rosenstein and Kantz. These algorithms are coded as lyap_r and lyap_k in the program respectively. It has been shown to give similar results in both lyap_r and lyap_k. It is stated that the small differences that can be neglected in the calculations are due to various calculation parameters such as embedding time, embedding delay, iteration number etc. The calculations in the fourth section are realized by using Kant algorithm (lyap_k).

2.2. Chaos Based Random Number Generator

An overview of the chaos-based random number generator that will be employed in the investigation is shown in Figure 1 [24]. The chaotic system has been utilized as an entropy source, as seen in Figure 1. The outputs of a chaotic system are computed for the chosen beginning conditions and control settings. The output values of the calculation are subjected to a threshold value function. Eq. (1) contains the thresholding function's mathematical model. The chaotic system outputs are converted to 0 or 1 values via this function. The resultant bit sequence was broken up into blocks of 8 bits each and transformed into values between 0 and 255.

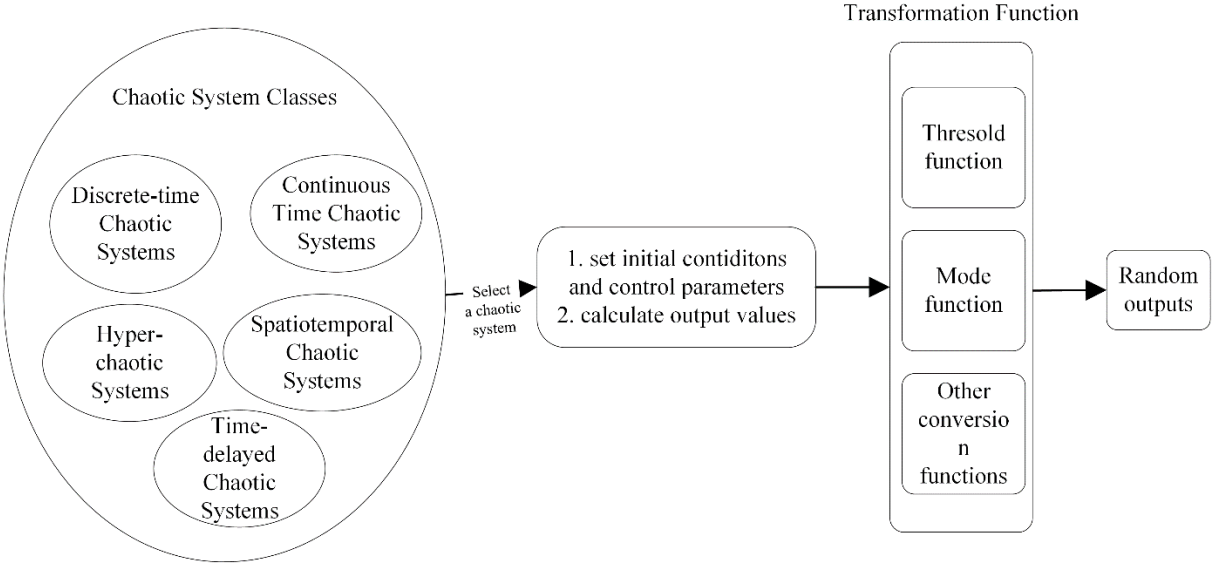

Figure 1. Overview of the chaos based random number generator

$$f_{threshold} = \begin{Bmatrix} x < 0.5 \rightarrow 0 \\ x \geq 0.5 \rightarrow 1 \end{Bmatrix} \quad (1)$$

The logistic map [22] has been used as the chaotic system in the study. The reason for choosing the logistics map is its simple structure. The simple structure will contribute to the faster operation of the generator. The mathematical model of the logistic map is given in Eq. (2). The map has only one initial condition and one control parameter.

$$x_{n+1} = a.x_n(1-x_n) \quad (2)$$

The pseudocode is included in Table 1 so that readers can better comprehend how the suggested algorithm functions as a random number generator.

The complexity of the entropy source (the chaotic system) is the fundamental tenet of chaos-based cryptography schemes. In other words, the quality of the random numbers will be higher in more complicated chaotic systems. Twelve different 1,000,00 lengths datasets have been generated using the proposed algorithm in the Table 1. Different initial conditions and control parameters have been used to obtain twelve different datasets.

Figure 2 shows the bifurcation diagram of the logistic map. As can be seen in Figure 2, when the control parameter a is set to between 0 and 3.5, the system shows periodic behavior. That is, when a value is selected in this range, the resulting logistic map outputs cannot be converted to random numbers by the proposed algorithm. Because values are not chaotic. The first six dataset used in the analyzes has been obtained for $a=3.0$, $a=3.1$, $a=3.2$, $a=3.3$, $a=3.4$, $a=3.3$ and $x_0=0.3$.

When a value between 3.5 and 4 is selected, the resulting logistic maps outputs can be converted to random numbers. Because, as can be seen from the bifurcation diagram, the outputs are unpredictable. The five dataset used in the study has been obtained in this direction $a=3.6$, $a=3,7$, $a=3.8$, $a=3.9$ and $a=4.0$ and $x_0=0.3$. When generating these dataset $x_0=0.3$ is selected randomly. The initial value is fixed to be consistent in all datasets.

Table 1. Chaos Based Random Number Generator.

Algorithm	Chaos Based Random Number Generator
Input	x_0 : initial condition of logistic map a : control parameter of logistic map n : length of sequence
Output	n -length sequence values ranging from 0-255

```
rng_sequence[1:n]
xold = x 0

for i in 1000
    xnew = a * xold* (1-xold)
end
for j in n
 value=""
 for k in 8
  xnew = a * xold* (1-xold)
  value=value+convert_str (fthreshold(xnew))
 end for
 rng_sequence[j]= convert_decimal (value)
end for
return rng_sequence
```

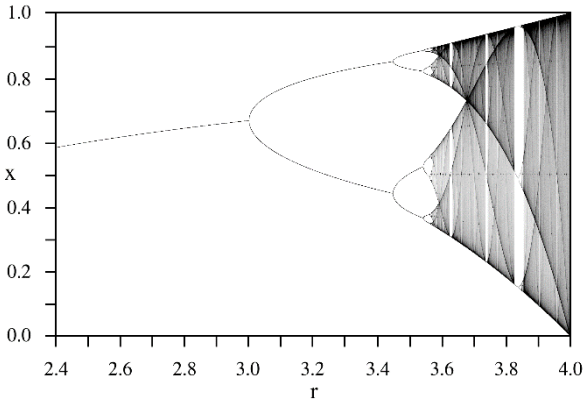

Figure 2. Bifurcation diagram of logistic maps

The final dataset illustrates the connection between chaos and randomness using optimization strategies. The best values for a and x_0 are looked at first. With the assistance of the differential evaluation optimization procedure, a and x_0 values have been established. In this direction, the last dataset has been obtained for a=4 and x_0=0.444369092261707.

3. Results

Randomness is related to probability, so that the properties of the random sequence can be defined as probabilistic. There are many statistical tests to evaluate the probabilistic properties of random numbers. These tests are used in the process of identifying samples that will ensure that the sequence is random.

Because there are many statistical tests, a generator that passes all tests cannot even say randomly. Because there is a possibility that the generator will fail for a new test. Therefore, the results of statistical tests should be interpreted well.

In order for a value to be defined random, it must be arbitrarily selected from the sequence and the values must be uniformly distributed.

However, when the distribution of a non-random sequence is examined, it does not seem to have a uniform distribution. Therefore, the probability distribution of the sequence is examined to test the randomness.
One of the simplest approaches to assess the randomness of a generator is the chi-square test. This test analyzes whether the data is uniformly distributed. If m random data is generated from the values between 0 and n, then it is expected that each value will be m/n units for the ideal situation. The chi-square values are calculated using Eq. (3).

$$X_c^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{3}$$

If the calculated chi-square value is smaller than the confidence values determined for the degree of freedom, the data may be random. 16 different values ranging from 0 to 15 are produced using RNG, therefore the degree of freedom is 16. The confidence values for this degree of freedom are given in Table 2.

Table 2. Confidence values for degree of freedom 16

DF	0.20	0.10	0.05	0.025	0.02	0.01	0.005	0.002	0.001
16	20.465	23.542	26.296	28.845	29.633	32.000	34.267	37.146	39.252

Calculated chi-square values for twelve different random sequences are given in Figure 3. The number of observed data from each value is given in Figure 4.

Name of Dataset	**Chi-square Value**
a=3 and x_0=0.3	3750000.0
a=3.1 and x_0=0.3	3750000.0
a=3.2 and x_0=0.3	3750000.0
a=3.2 and x_0=0.3	3749872.1
a=3.4 and x_0=0.3	3749904.1
a=3.5 and x_0=0.3	3749872.1
a=3.6 and x_0=0.3	1172184.7
a=3.7 and x_0=0.3	439080.7
a=3.8 and x_0=0.3	298875.8
a=3.9 and x_0=0.3	131710.9
a=4 and x_0=0.3	16.2
Optimum values	10.6

Figure 3. Chi-Square Values for Random Sequences

Dataset Name	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
a=3 and x_0=0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	250000
a=3.1 and x_0=0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	250000
a=3.2 and x_0=0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	250000
a=3.3 and x_0=0.3	0	0	0	0	0	249996	0	0	0	0	0	0	0	0	0	4
a=3.4 and x_0=0.3	0	0	0	0	0	0	0	0	0	0	249997	0	0	0	1	2
a=3.5 and x_0=0.3	0	0	0	0	0	0	0	0	0	0	3	0	0	0	249996	1
a=3.6 and x_0=0.3	0	0	0	0	0	0	0	0	0	0	113757	68262	0	0	67980	1
a=3.7 and x_0=0.3	0	0	0	0	0	23841	0	32213	0	0	23532	32108	0	32231	31691	74384
a=3.8 and x_0=0.3	0	0	0	0	0	23760	18754	27409	0	0	23358	45952	0	45518	27580	37669
a=3.9 and x_0=0.3	0	0	24617	0	14220	38559	15601	14276	0	24849	27916	29805	11052	18870	14217	16018
a=4 and x_0=0.3	15695	15373	15680	15455	15696	15458	15523	15649	15665	15656	15521	15729	15905	15672	15685	15638
Optimum values	15682	15723	15466	15454	15527	15536	15725	15578	15774	15717	15600	15523	15759	15723	15602	15611

Figure 4. The Number of Observed Data from Each Value

The most widely used statistical test package is NIST tests [25]. This analysis method, published as a test package, is accepted as the standard in many studies. There are 15 tests in NIST test package. These tests are "Monobit test, Frequency within block test, Runs_test, Longest run ones in a block test, Binary matrix rank test, Dft test, Non overlapping template matching test, Overlapping template matching test, Maurers universal test, Linear complexity test, Serial test, Approximate entropy test, Cumulative sums test, Random excursion test, Random excursion variant test".

NIST test results for twelve different dataset are given in Figure 5 and Figure 6. The S and F symbols in the figure indicate successful and unsuccessful test results, respectively. P symbol is the calculated probability value of the test. The test results revealed some problems of the NIST test package. The logistic map output values are periodic for control parameter less than 3.5. The periodicity of output of logistic map can be observed both in the bifurcation diagram in Figure 2 and in the distribution of numbers in Figure 4. However, NIST test results for random sequences generated for a = 3.3 and a = 3.4, are better than the sequences generated for a = 3.6, a=3.7, a=3.8, a=3.9. In other words, according to NIST test results, the values produced from periodic data are more random than the values produced from chaotic data. However, it is understood from the data distribution in Figure 4 that this claim is invalid. This indicates that the NIST test package cannot be used for analysis alone.

	selected initial conditions and control parameters											
Nist Test	**a=3.0 and x_0=0.3**		**a=3.1 and x_0=0.3**		**a=3.2 and x_0=0.3**		**a=3.3 and x_0=0.3**		**a=3.4 and x_0=0.3**		**a=3.5 and x_0=0.3**	
	S/F	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**
Monobit test	F	0	F	0	F	0	S	0.98723	S	0.99202	F	0
Frequency within block test	F	0	F	0	F	0	S	1	S	1	F	0
Runs test	F	0	F	0	F	0	F	0	F	0	F	0
Longest run ones in a block test	F	2.1e-203	F	2.13e-203'	F	2.7e-203	F	2.1e-159'	F	2.3e-159	F	3.2e-164
Binary matrix rank test	F	0	F	0	F	0	F	0	F	0	F	0
Dft test	F	0	F	0	F	0	F	0	F	0	F	0
Non overlapping template matching test	F	0	F	0	F	0	F	0	F	0	F	0
Overlapping template matching test	S	0.5839	S	0.5839	S	0.5839	S	0.5839	S	0.5839	S	0.5839
Maurers universal test	F	0.002398	F	0.0023989	F	0.0024	S	0.014128	S	0.014128	S	0.06119
Linear complexity test	S	1	S	1	S	1	S	1	S	1	S	1
Serial test	F	0	F	0	F	0	F	0	F	0	F	0
Approximate entropy test	F	0	F	0	F	0	F	0	F	0	F	0
Cumulative sums test	F	0	F	0	F	0	S	1	S	1	F	0
Random excursion test	F	2.7e-12	F	2.772e-12	F	2.7e-12	F	2.77e-12	F	2.7e-12	F	2.77e-12
Random excursion variant test	S	0.4795	S	0.81366	S	0.4795	S	0.4795	S	0.4795	S	0.13559
Total success rate	**3/15**		**3/15**		**3/15**		**7/15**		**7/15**		**4/15**	

Figure 5. Nist Test Results For Twelve Different Dataset Part 1

	selected initial conditions and control parameters											
Nist Test	**a=3.6 and x_0=0.3**		**a=3.7 and x_0=0.3**		**a=3.8 and x_0=0.3**		**a=3.9 and x_0=0.3**		**a=4.0 and x_0=0.3**		**Optimum values**	
	S/F	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**	**S/F**	**P-Value**
Monobit test	F	0	F	0	F	0'	F	0	S	0.67887	S	0,68034
Frequency within block test	F	0	F	0	F	0'	F	0	S	0.9832	S	0,79594
Runs test	F	0	F	0	F	0'	F	0	S	0.54995	S	0,94088
Longest run ones in a block test	F	3.2e-164	F	2.e-14	F	8.32e-28	F	0.005723	S	0.88981	S	0,48956
Binary matrix rank test	F	0	S	1	S	1	S	1	S	1	S	1
Dft test	F	0	F	0	F	3.6e-123	F	0	S	0.14708	S	0,08449
Non overlapping template matching test	F	0	F	0	F	0'	F	0	S	0.11967	S	0,68789
Overlapping template matching test	S	0.5839	S	0.5839	S	0.5839'	S	0.5839	S	0.5839	S	0,5839
Maurers universal test	S	0.18923	S	0.34316	S	0.54998'	S	0.89908	S	0.56887	S	0,57023
Linear complexity test	S	1	S	1	S	1'	S	1	S	1	S	1
Serial test	F	0	F	0	F	0 0'	F	0	S	0.76667	S	0,929425
Approximate entropy test	F	0	F	0	F	0'	F	0	S	0.7883	S	0,93674
Cumulative sums test	F	0	F	0	F	0 0'	F	0	S	1	S	1
Random excursion test	F	8.63e-19	F	2.77e-12	F	3.9e-14'	F	2.72e-16	F	0.003005	S	0,840948
Random excursion variant test	S	0.13559	S	0.41422	S	0.83117	S	0.81366	S	0.08453	S	0,739789
Total success rate	**4/15**		**5/15**		**5/15**		**5/15**		**14/15**		**15/15**	

Figure 6. Nist Test Results For Twelve Different Dataset Part 2

Table 3 shows the calculated Lyapunov exponential values for the outputs obtained by converting the chaotic system outputs to random numbers.

Table 3. Lyapunov Exponents For Rng Sequences

Name of Dataset	**Lyapunov exponents**
a=3 and x_0=0.3	does not compute
a=3.1 and x_0=0.3	does not compute
a=3.2 and x_0=0.3	does not compute
a=3.2 and x_0=0.3	does not compute
a=3.4 and x_0=0.3	does not compute
a=3.5 and x_0=0.3	does not compute
a=3.6 and x_0=0.3	0.23337
a=3.7 and x_0=0.3	0.23397
a=3.8 and x_0=0.3	0.26141
a=3.9 and x_0=0.3	0.29167
a=4 and x_0=0.3	0.30655
Optimum values	0.37462

The analysis has been shown that the NIST test results and the Lyapunov exponents calculated for both raw chaotic data outputs and random number sequence have been consistent. Another statement that the calculated Lyapunov exponential for a random number sequence is positive can be used as an indicator for the cryptographic quality of the generator.

4. Discussion

In the literature, it is seen that various statistical tests are used in the evaluation of many new chaos based cryptography proposals. The approaches such as histogram analysis, NPCR, UACI, and correlation analysis are used almost as standard in the analysis of image encryption algorithms. However, cryptanalysis studies in the literature have shown that many designs that pass these tests can be easily broken [26-31]. That is, these cryptanalysis have repeatedly shown that statistical analysis are necessary but not sufficient for the evaluation of chaos based designs. Therefore, new testing tools are needed to make more detailed assessments.

An important statistical analysis is known to be the NIST statistical randomness test suite. This analysis is seen as an important criterion in the evaluation of chaos based RNG studies. However, the analysis results in the section 3 showed that random numbers produced from non-chaotic data may show better statistical characteristics than random numbers produced from chaotic data. This is a significant disadvantage of the NIST test. The presence of a similar problem is shown on both monobit and chi-square tests.

Another problem with the NIST test suite is the number of bits required to perform the tests. 1000000 bits are required to evaluate the statistical properties of the generator. This is a very large number for cryptography applications. Because it is often taken into account that the generators are used in the key planning algorithm of cryptographic design, short length bit sequences like 256 bits (AES) or 1024 bits (RSA) are needed.

It has been revealed that these problems can be eliminated by the proposed new analysis method. The analysis results can be interpreted as follows.

- Whether it is produced from periodic or chaotic data, it has been shown to have negative Lyapunov implications if the generated sequence do not meet the randomness requirements.
- The fact that the Lyapunov exponents can be calculated in short-length sequences has eliminated the 1000000-bit requirement problem.
- The simplicity of the calculations increases the applicability of the method.

5. Conclusions

Theoretically, cryptography and chaos have a close link. The two fields' primary traits are similar to one another. The creation of new cryptographic protocols has always taken advantage of this tight link. This study has demonstrated how to exploit this relationship to decrypt chaos-based encryption schemes. The generated data can be used as a key or seed value in similar chaos-based encryption algorithms [32].

To be considered secure, a cryptographic design is assumed to meet the conditions for confusion and dispersion.

According to some, the Lyapunov exponential can be used to measure these criteria. An analytical tool for quantifying chaos is the Lyapunov exponent. Given the connection between chaos and cryptography, it has been proposed that mixing and diffusion requirements can be verified by the presence of chaos.
This study has demonstrated that Lyapunov exponents can be used to examine random number generators. The successful analytical results supported the potential of the suggested approach to serve as a test tool for cryptography design. It has also been demonstrated that a number of issues with the NIST test suite can be fixed.

Acknowledgements

This study is supported by the TUBITAK Project Number 120e444.

References

[1] Strogatz SH. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering. Boca Raton, Fl Westview Press, 2014.
[2] Özkaynak F. Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn. 2018; 92: 305–313.
[3] Li C, Zhang Y, Xie EY. When an attacker meets a cipher-image in 2018: A year in review. Journal of Information Security and Applications 2019; 48: 102361.
[4] Özkaynak F. Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals. 2017 International Conference on Computer Science and Engineering (UBMK); 2017; Antalya,Turkey. pp. 621-624
[5] Liu X, Song Y, Jiang G. Hierarchical Bit-Level image encryption based on Chaotic Map and Feistel network. Int. J. Bifurcation Chaos 2019; 29: 1950016.
[6] Shen Q, Liu Y. A novel digital image encryption algorithm based on orbit variation of phase diagram. Int. J. Bifurcation Chaos 2017; 27(13): 1750204.
[7] Yin Q, Wang C. A new chaotic image encryption scheme using Breadth-First search and dynamic diffusion. Int. J. Bifurcation Chaos 2018; 28(4): 1850047.
[8] Ye G, Pan C, Huang X, Zhao Z, He J. A chaotic image encryption algorithm based on information entropy. Int. J. Bifurcation Chaos 2018; 28(1): 1850010.
[9] Chenaghlu MA, Jamali S, Nikzad-Khasmakhi N. A novel keyed parallel hashing scheme based on a new chaotic system. Chaos, Solitons & Fractals 2016; 87: 216–25.
[10] Li Y, Li X. Chaotic hash function based on circular shifts with variable parameters. Chaos, Solitons & Fractals 2016; 91: 639–48.
[11] Solami EA, Ahmad M, Volos C, Doja MN, Beg MMS. A new hyperchaotic System-Based design for efficient bijective Substitution-Boxes. Entropy 2018; 20: 525.
[12] Tanyıldızı E, Özkaynak F. A new chaotic S-Box generation method using parameter optimization of one dimensional chaotic maps. IEEE Access 2019; 7: 117829–38.
[13] Kanso A, Ghebleh M. A fast and efficient chaos-based keyed hash function. Commun. Nonlinear Sci. Numer. Simul. 2013; 18: 109–23.
[14] Lambić D, Nikolić M. Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn. 2017; 90: 223–32.
[15] Sahari ML, Boukemara I. A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. Nonlinear Dyn. 2018; 94: 723–44.
[16] Zambrano-Serrano E, Munoz-Pacheco JM, Campos-Cantón E. Chaos generation in fractional-order switched systems and its digital implementation. AEU Int. J. Electron. Commun. AEU International 2017; 79: 43–52.
[17] Avaroğlu E. Pseudorandom number generator based on Arnold cat map and statistical analysis. Turk. J. Electr. Eng. Comput. Sci. 2017; 25: 633–43.
[18] Avaroğlu E, Koyuncu İ, Özer AB, Türk M. Hybrid pseudo-random number generator for cryptographic systems. Nonlinear Dyn. 2015; 82: 239–48.
[19] Türk Ö. FPGA simulation of chaotic tent map-based S-Box design. Int. J. Circuit Theory Appl. 2022; 50: 1589–603.
[20] Koyuncu İ, Özcerit AT, Pehlivan I, Avaroğlu E. Design and implementation of chaos based true random number generator on FPGA. 22nd Signal Processing and Communications Applications Conference; 2014; Trabzon, Turkey. pp. 236-239
[21] Hilborn RC. Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers. New York: Oxford Univ. Press, 2000.
[22] Sprott JC. Chaos and Time-Series Analysis. USA : Oxford University Press, 2003.
[23] Kantz H, Schreiber T. Nonlinear Time Series Analysis. Technometrics 2005; 47: 381.
[24] Özkaynak F. Cryptographically secure random number generator with chaotic additional input. Nonlinear Dyn. 2014; 78: 2015–20.
[25] Rukhin AL, Soto J, Nechvatal J, Smid ME, Barker EB. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications., 2010.
[26] Arroyo D, Hernández F, Orue AB. Cryptanalysis of a Classical Chaos-Based Cryptosystem with Some Quantum Cryptography Features. Int. J. Bifurcation Chaos 2017; 27: 1750004.

[27] Li C, Lin D, Lu J, Hao F. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. IEEE MultiMedia 2018; 25: 46–56.
[28] Li C, Lo K-T. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. 2011; 91: 949–54.
[29] Li S, Li C, Chen G, Bourbakis NG, Lo K-T. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. Image Commun. 2008; 23: 212–23.
[30] Lin Z, Yu S, Feng X-L, Lu J. Cryptanalysis of a chaotic stream cipher and its improved scheme. Int. J. Bifurcation Chaos 2018; 28: 1850086.
[31] Muhammad ZMZ, Özkaynak F. Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique. IEEE Access 2019; 7: 99945–53.
[32] Ari A. CDIEA: Chaos and DNA based Image Encryption Algorithm. TJST 2023; 18: 261–73.