IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 39, No. 5, October, 2022, pp. 1647-1653
Journal homepage: http://iieta.org/journals/ts

Chaos Based Pseudo Random Bit Generator Design and Its Application in Secure Image Encryption

Esra İnce, Barış Karakaya*, Mustafa Türk

Faculty of Engineering, Department of Electrical-Electronics Engineering, Firat University, Elazığ 23119, Turkey

Corresponding Author Email: bkarakaya@firat.edu.tr

https://doi.org/10.18280/ts.390522

Received: 13 June 2022
Accepted: 20 September 2022

Keywords:
chaotic map, fixed-point conversion, post-processor, random number bit generator, statistical tests

ABSTRACT

Security and privacy problems in communication systems and social media platforms where digital image/video are shared almost always, have attracted researchers interest on information security. Starting from this point of view, a novel one-dimensional chaotic maps based pseudo random bit generator is proposed to make a significant contribution to the literature about protection of personal data in any network. Electronic circuit realizations of Logistic and Tent maps as entropy source are designed on Orcad-Pspice environment and state variables are inputted to novel post-processor algorithm. The rest of main blocks of proposed pseudo random bit generator design are built up fixed-point binary conversion algorithm, XOR processor and H function post-processor. The generated pseudo random bit series are tested by using NIST 800.22 statistical test suite and applied to color image encryption in order to show the effectiveness of proposed design. Cryptanalysis processes such as histogram, NPCR-UACI and correlation analysis are demonstrated. Analysis results show that the proposed design can be used successfully in many secure communication and media transmission applications.

1. INTRODUCTION

Nowadays, image, text and video encryption technology has a great importance for social media, communication systems and cyber-security systems. Especially, the secure communication between most important units of governments such as military are face to enemy attacks. Due to this intensification of sharing digital information, images and videos through any communication environment, the most important subject to be concentrated is secure communication [1-4]. Therefore, researchers show great interest in encryption techniques to be ensure on secure communication. Since all encryption techniques require private key value or bits, the security of a cryptographic system relies on the private key. Compared with traditional encryption algorithms, chaos-based hardware architectures have demonstrated outstanding performance with proven true random bit generation as private key and ability of increased security and privacy of the communication system [5-8]. In this study, it is aimed to ensure information confidentiality and secure communication especially in military areas by using chaotic hardware circuit structures based encryption methods and algorithms.

In the literature, there are so many studies on chaos based image, video and text encryption applications. Especially, chaotic map based encryption techniques have been utilized by several researchers. A modified Logistic map based encryption is proposed by Han [9] in 2019 to overcome the problems of small key space and poor security. An image cipher algorithm is proposed by Kumar et al. [10] in 2022 that uses Logistic and Arnold's cat maps by shuffling the pixels of an input color image. There are also several studies using electronic circuit realizations of chaotic dynamical systems as entropy source such as the study [11] proposed by Volos et al. in 2013, where true random bits are generated from the synchronization results of nonlinear Chua's like autonomous circuit and bits sequence has then been used to encrypt and decrypt gray-scale images. Chaotic time-series obtained from a non-equilibrium system are used to construct S-boxes and develop an image encryption application by Wang et al. [12] in 2019. Furthermore, researchers proposed to use different chaotic dynamical systems as entropy source; circuit realization, control design and image encryption application of their proposed system such as extended Lü system [13], autonomous RLCC-Diodes-Opamp chaotic oscillator [14, 15], modified Chua's circuit [16], a new chaotic jerk system [17] and chaotic one dimensional maps [18-24].

There are also so many studies using Substitution boxes (S-boxes) [21, 25, 26] and post-processors to provide the diffusion and permutation of the image pixels such as XOR [27, 28], H function [29], Von Neumann corrector [30, 31] and so on. In this study, permutation and diffusion processes for encrypted image with generated random bits are provided by using fixed-point number conversion, XOR and H function post-processor all together. In the proposed technique, the state variable values of Logistic and Tent maps are converted to their fixed-point binary equivalence, then the bit streams for each state variables are inputted to XOR logical function, sampling and H function respectively in order to generate statistically random bits.

The main objective of this paper is to generate pseudo random bit from the electronic circuit realization of Logistic and Tent maps. The electronic circuits designed and simulated on Orcad-Pspice environment. In order to implement the electronic circuits of chaotic map equations, general-purpose operational amplifiers and special integrated circuits (IC) such as AD633 and LF398 are used.

Herewith this introduction, chaotic Logistic and Tent maps are defined and the trends of their state variables are given in Section 2. In Section 3, electronic circuit realizations of Logistic and Tent maps are designed and map equations are detailed with the equivalent form active and passive circuit elements. The main blocks of proposed pseudo random bit generator (PRBG) design; entropy source, fixed-point binary conversion algorithm, XOR processor, bit accumulator, sampling, H function post-processor and statistical test results are detailed in Section 4. The generated pseudo random bit (PRB) series are applied to color image encryption in order to show the effectiveness of PRBG and cryptanalysis processes such as histogram, NPCR-UACI and correlation analysis are demonstrated in Section 5. At the end, final section concludes the paper.

2. CHAOTIC LOGISTIC AND TENT MAPS

In this section, definitions of Logistic map and Tent map are detailed with the parameters and dynamics of systems. The Logistic and Tent maps are 1D chaotic maps and the state variable of each shows various dynamic properties with the equations below;

$$x_{log(n+1)} = r * x_{log(n)} * \left(1 - x_{log(n)}\right) \quad (1)$$

$$x_{tent(n+1)} = \begin{cases} a * x_{tent(n)} & x_{tent(n)} < 0.5 \\ a * \left(1 - x_{tent(n)}\right) & x_{tent(n)} \geq 0.5 \end{cases} \quad (2)$$

where, r and a are control parameters of maps, chaotic behavior is obtained $r \in [3.5, 4]$ and $a \in [1.5, 2]$ for each map respectively. The initial condition of state variable varies between the same value, $x \in [0, 1]$, for both Logistic map and Tent map. The variation of state variables is given in Figure 1 for r=3.9, a=1.99 under the same initial condition for both is $x(0)$=0.61.

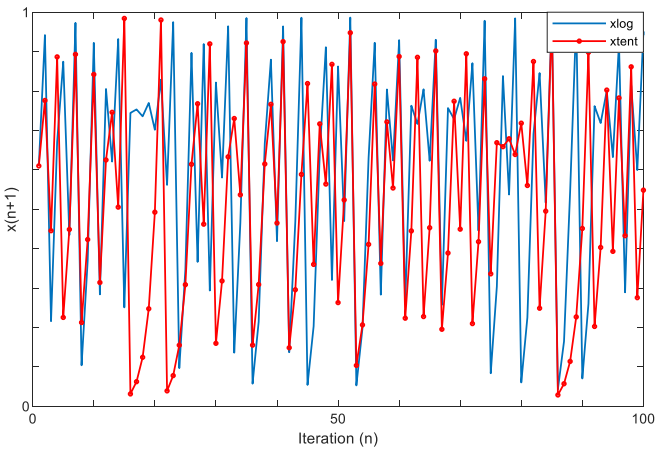

Figure 1. The trend of state variables of Logistic (xlog) and Tent (xtent) maps

As it is clearly appeared in Figure 1 that there is a noise like behavior from the output of each chaotic map. Recently, chaotic maps are studied much in image/video encryption applications because their simple equations and very sensitive structure to initial conditions.

3. ELECTRONIC CIRCUIT REALIZATIONS OF CHAOTIC MAPS

Starting from the mathematical model of any linear or nonlinear system, it is always possible and easy to realize an equivalent electronic circuit that obeys to the same set of equations [32]. The aim of this study is to generate secure pseudo random bits using electronic circuit realizations of 1D chaotic maps. The circuitries are designed on Orcad-Pspice environment to obtain the variation of state variables iteratively. Most researchers, studying on chaotic electronic circuits, design the circuits by using active circuit elements such as operational amplifier, analog multiplier, multiplexer and standard passive circuit elements such as resistor, capacitor and so on. From the mathematical model of chaotic systems to the electronic circuit, the most important active circuit element is operational amplifier. Especially for the discrete chaotic systems i.e. chaotic maps, sample and hold integrated circuit (special operational amplifiers) is very essential. The electronic circuit realizations of Logistic and Tent maps are designed and simulated on Orcad-Pspice environment as given in Figures 2 and 3 according to the observations made during the numerical analysis on MATLAB.

In the design stage of electronic circuits, general purpose operational amplifiers are used. On the other hand, LF398 integrated circuit is used for sample and hold operations because the chaotic maps have discrete dynamical equations. In order to implement the mathematical model of chaotic maps, classical definitions of op-amps and the mathematical equations of special integrated circuits such as AD633 and LF398 have to be analyzed.

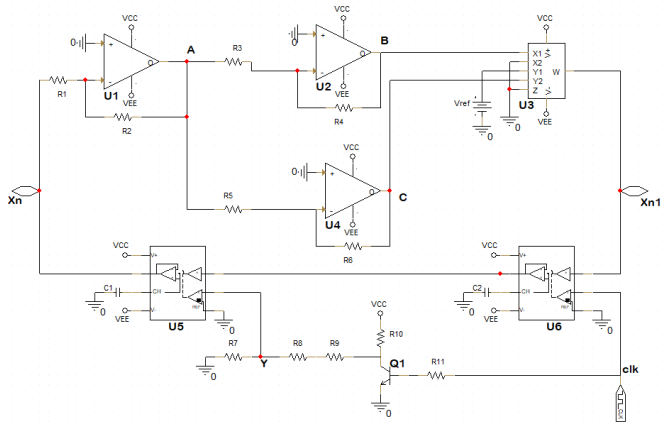

Figure 2. The electronic circuit realization of logistic map on Orcad-Pspice environment

The LF398 is a monolithic sample and hold circuit that is a unity-voltage gain follower that is used in both Logistic and Tent experimental circuits. A hold capacitor is connected output pin of LF398 to obtain sampled voltage on it. TTL compatible square wave (*clk*) signal provided from the signal generator is used to trigger the first LF398 (on the right). The second LF398 (on the left) is triggered by the logic inverse of this square wave (*Y*). A common emitter NPN bipolar 2N2222 transistor is used to provide inverse of square wave. The initial value for circuit operation is applied to the hold capacitor connected to the first LF398 in both electronic circuits. The new value of state variable (*Xn1*) is generated in once every period of the TTL signal. The AD633 is a functionally

complete analog multiplier, includes high impedance, differential X and Y inputs, and a high impedance summing input (Z). The transfer function of the AD633 IC used in the electronic circuit of the Logistic map is as follow:

$$W = \frac{(X1-X2)*(Y1-Y2)}{10V} + Z \quad (3)$$

where, W is the output of multiplier.

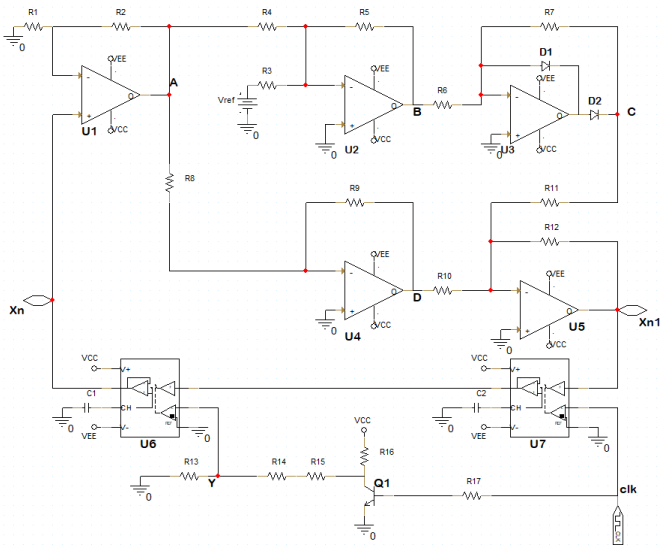

Figure 3. The electronic circuit realization of Tent map on Orcad-Pspice environment

The list of experimental circuit elements is given in Table 1 while the values of all passive circuit elements and voltage supplies are detailed in Table 2.

Table 1. The list of experimental circuit elements used in electronic circuits

Tent Map		Logistic Map	
U_1, U_2, U_3, U_4, U_5	TL082	U_1, U_2, U_4	TL082
U_6, U_7	LF398	U_3	AD633
Q1	2N2222	U_5, U_6	LF398
D_1, D_2	1N4148	Q_1	2N2222

Table 2. The values of circuit elements used in electronic circuits

Tent map		Logistic map	
R_1	100 kΩ	R_1, R_3, R_5, R_6, R_{11}	10 kΩ
R_2, R_3, R_4, R_5, R_6, R_8, R_{10}, R_{11}, R_{12}, R_{16}	1 kΩ	R_2	50 kΩ
R_7	4 kΩ	R_4	15.6 kΩ
R_9	2.1 kΩ	R_7, R_8, R_9,	2.2 kΩ
R_{13}, R_{14}, R_{15}	2.2 kΩ	R_{10}	1 kΩ
R_{17}	10 kΩ	C_1, C_2	0.01 µF
C_1, C_2	0.01 µF	V_{ref}	5 V
V_{ref}	-0.5 V	V_{CC}	+15 V
V_{CC}	+15 V	V_{EE}	-15 V
V_{EE}	-15 V		

The conversion of mathematical models of chaotic maps to electronic circuits regarding basic circuit rules and by using Eq. (1), (2) and (3), Figure 2 and Figure 3 can be analyzed. The output ($Xn1$) of Logistic map related to the input (Xn) is analyzed node by node through the following equations:

$$A = -\frac{R_2}{R_1}X_n \quad (4)$$

$$B = -\frac{R_4}{R_3}A \quad (5)$$

$$C = -\frac{R_6}{R_5}A \quad (6)$$

$$X_{n1} = \frac{B(V_{ref}-C)}{10} \quad (7)$$

$$X_{n1} = \frac{\frac{R_4R_2}{R_3R_1}X_n\left(V_{ref}-\frac{R_6R_2}{R_5R_1}X_n\right)}{10} \quad (8)$$

$$X_{n1} = \frac{1}{10}\frac{R_4}{R_3}\frac{R_2}{R_1}X_nV_{ref} - \frac{1}{10}\frac{R_4}{R_3}\frac{{R_2}^2}{{R_1}^2}\frac{R_6}{R_5}{X_n}^2 \quad (9)$$

$$X_{n1} = 3.9X_n(1-X_n) \quad (10)$$

where, $Xn1$ stands for next iterative value of Logistic map while Xn is actual. The output ($Xn1$) of Tent map related to the input (Xn) is analyzed node by node through the following equations:

$$A = \left(\frac{R_2}{R_1}+1\right)X_n \quad (11)$$

$$B = -\frac{R_5}{R_4}A - \frac{R_5}{R_3}V_{ref} \quad (12)$$

$$C = -\frac{R_7}{R_6}B \quad (13)$$

$$D = -\frac{R_9}{R_8}A \quad (14)$$

$$X_{n1} = -\frac{R_{12}}{R_{10}}D - \frac{R_{12}}{R_{11}}C \quad (15)$$

$$X_{n1} = \frac{R_{12}}{R_{10}}\frac{R_9}{R_8}\left(\left(\frac{R_2}{R_1}+1\right)X_n\right) + \frac{R_{12}}{R_{11}}\frac{R_7}{R_6}\left(-\frac{R_5}{R_4}\left(\left(\frac{R_2}{R_1}+1\right)X_n\right) - \frac{R_5}{R_3}V_{ref}\right) \quad (16)$$

$$X_{n1} = \frac{R_{12}}{R_{10}}\frac{R_9}{R_8}\frac{R_2}{R_1}X_n + \frac{R_{12}}{R_{10}}\frac{R_9}{R_8}X_n + \frac{R_{12}}{R_{11}}\frac{R_7}{R_6}\left(-\frac{R_5}{R_4}\frac{R_2}{R_1}X_n - \frac{R_5}{R_4}X_n - \frac{R_5}{R_3}V_{ref}\right) \quad (17)$$

$$X_{n1} = \frac{R_{12}}{R_{10}}\frac{R_9}{R_8}\frac{R_2}{R_1}X_n + \frac{R_{12}}{R_{10}}\frac{R_9}{R_8}X_n - \frac{R_{12}}{R_{11}}\frac{R_7}{R_6}\frac{R_5}{R_4}\frac{R_2}{R_1}X_n - \frac{R_{12}}{R_{11}}\frac{R_7}{R_6}\frac{R_5}{R_4}X_n + \frac{R_{12}}{R_{11}}\frac{R_7}{R_6}\frac{R_5}{R_3}V_{ref} \quad (18)$$

$$X_{n1} = \frac{R_{12}}{R_{10}}\frac{R_9}{R_8}X_n - \begin{cases} 0, & X_n < \frac{R_4}{2R_3} \\ \frac{R_{12}}{R_{11}}\frac{R_7}{R_6}\left(\frac{R_5}{R_4}X_n - \frac{R_5}{2R_3}\right), & X_n \geq \frac{R_4}{2R_3} \end{cases} \quad (19)$$

where, $Xn1$ stands for next iterative value of Tent map while Xn is actual. As the all resistor values are taken into account in Eq. (19), the value of the bifurcation parameter a can be fixed at certain values by simply adjusting the R_7 and R_9 resistor connected to feedback resistor in the operational amplifiers of U_3 and U_4. The relationship between the resistors R_7 and R_9 with the value of $a \cong 2$ and the simplest equation for Tent map can be obtained in Eq. (20) below.

$$X_{n1} = \begin{cases} aX_n & X_n < \frac{1}{2} \\ a(1 - X_n) & X_n \geq \frac{1}{2} \end{cases} \quad (20)$$

As it is clearly seen in the equations above, the electronic circuit realization of any mathematical models can be installed by using basic rules of common electronic components and special integrated circuits. The trend of the state variables of discrete chaotic maps are illustrated in Figure 4 for the same initial condition value of 0.61 V.

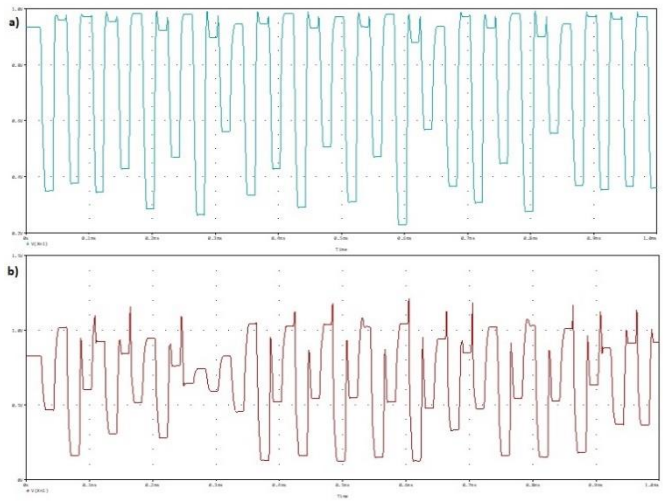

Figure 4. The trend of the state variable of a) Logistic map and b) Tent map for the same initial condition value of 0.61 V

The trends of output for each chaotic maps are discrete and noise-like behavior can be observed. The new value of state variables is produced iteratively at every 20 µs which is the period of trigger digital signal (*clk*).

4. PROPOSED PSEUDO RANDOM BIT GENERATOR DESIGN AND STATISTICAL TESTS

The aim of this study is to generate secure pseudo random bits using electronic circuit realizations of 1D discrete chaotic maps. The proposed PRBG design consists of discrete Logistic and Tent maps as entropy source, fixed-point binary conversion algorithm, XOR processor, bit accumulator, sampling and H function post-processor as illustrated in Figure 5. The values of state variables are imported to MATLAB platform in order to apply fixed-point binary conversion algorithm and the rest of the proposed design processes.

The design has chaotic discrete maps as entropy source that are simulated on Orcad-Pspice environment in order to obtain almost 1 million data. The simulation results are 995654 fractional numbers in double format for each chaotic map. In order to provide diffusion requirement of random bit generator securely, the value of state variables is converted to binary form by using Q1.15 unsigned fixed-point fractional number representation format where most significant bit is discarded because of state variables of Logistic and Tent maps are in the range of [0,1]. The whole diffusion processes (conversion, XOR, sampling, H function post-processor) are illustrated in Figure 5 and detailed by giving the pseudo code for each process in Table 3.

The pseudo random bit stream is in 7467345-bit length that is generated by using the chaotic maps as entropy source. In order to show effectiveness of the proposed PRBG design, the bit stream is subjected to statistical randomness tests. In to analyze statistically randomness of any number or bit stream can be tested by using NIST 800.22 test suite that is explained in details in the study of Rukhin et al. [33]. In this study, statistical randomness tests of generated bits are carried out by the NIST 800.22 test suite and Table 4 demonstrates these statistical tests results.

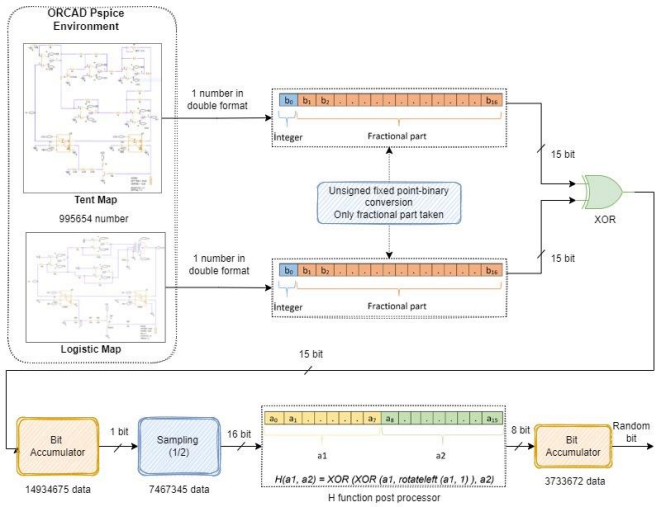

Figure 5. Block diagram of the proposed PRBG design

Table 3. The pseudo-code of fixed-point conversion, XOR & sampling and H function post-processor.

Algorithm 1: Q1.15 unsigned fixed-point fractional number conversion of chaotic map outcomes (**fixed-point binary conversion**)
Input: State variables of chaotic Logistic (xlog) and Tent (xtent) maps generated on Orcad-Pspice environment
Output: Unsigned fixed-point fractional numbers in 15-bit length for each decimal number input
q=quantizer ('ufixed', [16 15])
for i = 1: 1: 995654
xlog_f = num2hex (q, xlog (:));
xtent_f = num2hex (q, xtent (:));
xlog_frc = hex2bin (q, xlog_f);
xtent_frc = hex2bin (q, xtent_f);
x_l_f (i) = xlog_frc (2:16);
x_t_f (i) = xtent_frc (2:16);
end

Algorithm 2: Process for XOR function and sampling by 2 (**XOR logic operation and sampling**)
Input: 995654 data each one of is in 15-bit length
Output: XORed and sampled data in 7467345-bit length
for i=1: 2: 995654
*xlogtent ((i-1) * 15+1: i*15, 1) =XOR (x_l_f (i), x_t_f (i));*
end

Algorithm 3: H function as a post-processor
Input: Data in 7467345-bit length
Output: Pseudo random bit (PRB) stream in 7467345-bit length
for i = 1: 1: 7467345
*x_hash = xlogtent ((i-1) * 16 + 1: i*16);*
a1 = x_hash (1:8);
a2 = x_hash (9:16);
*PRB ((i-1) * 8+1: i * 8) = XOR (XOR (a1, rotateleft (a1,1)), a2);*
end

Table 4. Statistical test results of the proposed PRBG design outputs

NIST Tests (3733672 bit)	PRB1 (first 1572864 bit)	Result	PRB2 (last 1572864 bit)	Result
Frequency (monobit) Test	0.5541	**Passed**	0.4819	**Passed**
Frequency Test within a Block	0.3318	**Passed**	0.62	**Passed**
Runs Test	0.5528	**Passed**	0.2244	**Passed**
Test for the Longest Run of Ones in a Block	0.605	**Passed**	0.711	**Passed**
Binary Matrix Rank	0.0565	**Passed**	0.5931	**Passed**
Discrete Fourier Transform Test	0.6369	**Passed**	0.7427	**Passed**
Non-overlapping Template Matching Test	0.1652	**Passed**	0.0634	**Passed**
Overlapping Template Matching Test	0.2109	**Passed**	0.7234	**Passed**
Maurer's Universal Statistical Test	0.5814	**Passed**	0.5411	**Passed**
Linear Complexity Test	0.1394	**Passed**	0.091	**Passed**
Serial Test 1/2	0.0231 / 0.277	**Passed**	0.525 / 0.4394	**Passed**
Lempel Ziv Test	77623 / 2 / 1	**Passed**	77620 / 2 / 1	**Passed**
Approximate Entropy Test	0.013	**Passed**	0.5903	**Passed**
Cumulative Sums Test	0.8263	**Passed**	0.2575	**Passed**
Random Excursions Test	0.0941	**Passed**	0.3048	**Passed**
Random Excursions Variants Test	0.0466	**Passed**	0.3286	**Passed**

According to Table 4, it can be clearly seen that generated pseudo random bit series passed all tests successfully. After proving the statistically randomness of bit stream, an image encryption application is carried out with the analysis and results to show the effectiveness of the proposed PRBG design.

5. IMAGE ENCRYPTION APPLICATION, ANALYSIS AND RESULTS

The image encryption stage of this study consists of two application phases. In first, the bit stream obtained proposed pseudo bit generator design is split into two parts each has 1572864 bit (PRB1 and PRB2) and statistically random as proved in Table 4. Then, each random bit stream is inputted to XOR function with one original test image. Since the size of original test image is 256x256 in RGB format, required random key bit length is determined as 256 rows x 256 columns x 3 channels x 8 bit = 1572864 bit. The original test image, encrypted image with PRB1 and encrypted image with PRB2 which are in the same size are illustrated in Figure 6.

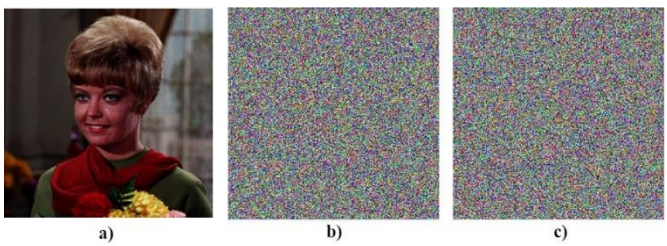

Figure 6. a) The original test image b) Encrypted image with PRB1 c) Encrypted image with PRB2

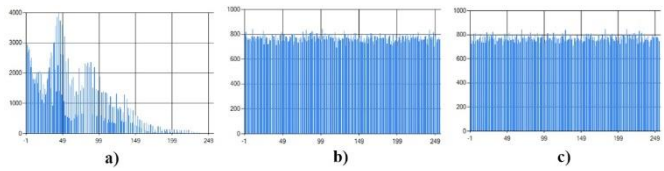

Figure 7. Histogram analysis for a) original image b) encrypted image with PRB1 c) encrypted image with PRB2

Most of researchers studying on image encryption use cryptanalysis processes in order to show the effectiveness of their proposed random bit designs such as histogram, NPCR-UACI and correlation analysis. Histogram analysis is the graphical measure of the distribution of pixel values on an image. Especially for the image encryption applications, the algorithm of histogram analysis should follow two criteria. First, histograms of original and encrypted images must differ from significantly one to another. Second, the distribution of pixel values in encrypted image should be uniform [34, 35]. The histograms of original test image, encrypted image with PRB1 and encrypted image with PRB2 are given in Figure 7.

When the histogram plots are examined, it is seen that the original test image and encrypted image with both PRB1 and PRB2 are completely different from each other. Also, the distribution of pixel values in encrypted images are uniform.

In addition to the histogram analysis, there are also two statistical tests which provide effectiveness of encryption algorithm on image encryption applications. These measurements are Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) tests where a value of 0.99 for the NPCR test and a value of 0.33 for UACI test are considered as success criteria. The calculated NPCR and UACI values for the encrypted image shown in Figure 6 are 0.995961507161458 and 0.334804133495292, respectively. It is clearly observed that the calculated test results are very close to the success criteria.

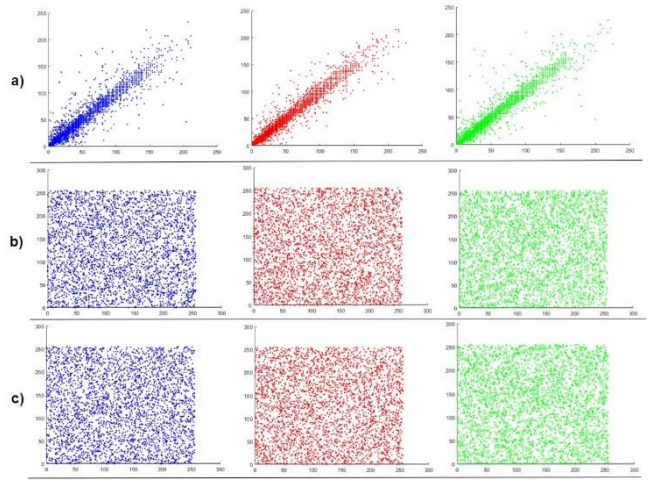

Figure 8. Correlation distribution of a) the original test image b) encrypted image with PRB1 and c) encrypted image with PRB2; along diagonal, horizontal and vertical direction where each one of them is indicated as a column, respectively

Correlation analysis shows the correlation of adjacent pixels in an image along diagonal (D), horizontal (H), vertical (V) directions. This analysis tool is also used to verify the inferences the correlation distributions of the original and encrypted images. The correlation distribution of the original test image is generally high. Therefore, the encryption algorithm or design must remove the correlation between adjacent pixels as much as possible [36]. Figure 8 shows the correlation distribution of original test image in Figure 6 (a) and the encrypted images with the PRB1 and PRB2 given in Figure 6 (b) and Figure 6 (c), respectively.

All the results of the statistical tests and analyses reveal that the pseudo random bit generated from chaotic discrete maps can be used in image/media encryption applications securely. Furthermore, the proposed image encryption application passes all the both statistical and differential attack tests.

6. CONCLUSIONS

The proposed design has two 1D chaotic maps and their electronic circuit on Orcad-Pspice environment to observe the effectiveness of chaos based image encryption systems. The design has passed all the statistical tests successfully and the metrics of cryptanalysis have been verified. The proposed post-processor blocks are built up fixed-point binary conversion algorithm, XOR processor and H function post-processor. Considering the results obtained and given in the previous sections, it can be concluded that the proposed design can be used successfully in communication and media transmission systems as it has complex algorithms, trustable diffusion and permutation processes.

As a future study, it is aimed to design a secure hardware-based image/video encryption system for military unmanned aerial vehicles by using a combination of chaotic dynamic system and user biometric data.

ACKNOWLEDGMENT

This work is supported by The Scientific and Technological Research Council of Turkey (TUBITAK) Project Number: 121E003 and also produced from the part of Esra İnce's Doctoral Thesis.

REFERENCES

[1] Yalcin, M.E., Suykens, J.A., Vandewalle, J. (2004). True random bit generation from a double-scroll attractor. IEEE Transactions on Circuits and Systems I: Regular Papers, 51(7): 1395-1404. https://doi.org/10.1109/TCSI.2004.830683

[2] Karakaya, B., Gülten, A., Frasca, M. (2019). A true random bit generator based on a memristive chaotic circuit: Analysis, design and FPGA implementation. Chaos, Solitons & Fractals, 119: 143-149. https://doi.org/10.1016/j.chaos.2018.12.021

[3] Garipcan, A.M., Erdem, E. (2020). A TRNG using chaotic entropy pool as a post-processing technique: analysis, design and FPGA implementation. Analog Integrated Circuits and Signal Processing, 103(3): 391-410. https://doi.org/10.1007/s10470-020-01605-0

[4] Kaur, M., Kumar, V. (2020). A comprehensive review on image encryption techniques. Archives of Computational Methods in Engineering, 27(1): 15-43. https://doi.org/10.1007/s11831-018-9298-8

[5] Yasser, I., Mohamed, M.A., Samra, A.S., Khalifa, F. (2020). A chaotic-based encryption/decryption framework for secure multimedia communications. Entropy, 22(11): 1253. https://doi.org/10.3390/e22111253

[6] Karakaya, B., Çelik, V., Gülten, A. (2017). Chaotic cellular neural network-based true random number generator. International Journal of Circuit Theory and Applications, 45(11): 1885-1897. https://doi.org/10.1002/cta.2374

[7] Çavuşoğlu, Ü., Kaçar, S., Zengin, A., Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics, 92(4): 1745-1759. https://doi.org/10.1007/s11071-018-4159-4

[8] Koyuncu, İ., Tuna, M., Pehlivan, İ., Fidan, C.B., Alçın, M. (2020). Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator. Analog Integrated Circuits and Signal Processing, 102(2): 445-456. https://doi.org/10.1007/s10470-019-01568-x

[9] Han, C. (2019). An image encryption algorithm based on modified logistic chaotic map. Optik, 181: 779-785. https://doi.org/10.1016/j.ijleo.2018.12.178

[10] Kumar, K., Roy, S., Rawat, U., Malhotra, S. (2022). IEHC: An efficient image encryption technique using hybrid chaotic map. Chaos, Solitons & Fractals, 158: 111994. https://doi.org/10.1016/j.chaos.2022.111994

[11] Volos, C.K., Kyprianidis, I.M., Stouboulos, I.N. (2013). Image encryption process based on chaotic synchronization phenomena. Signal Processing, 93(5): 1328-1340. https://doi.org/10.1016/j.sigpro.2012.11.008

[12] Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., Pham, V.T., Jafari, S., Nguyen, X.Q. (2019). S-box based image encryption application using a chaotic system without equilibrium. Applied Sciences, 9(4): 781. https://doi.org/10.3390/app9040781

[13] Lai, Q., Norouzi, B., Liu, F. (2018). Dynamic analysis, circuit realization, control design and image encryption application of an extended Lü system with coexisting attractors. Chaos, Solitons & Fractals, 114: 230-245. https://doi.org/10.1016/j.chaos.2018.07.011

[14] Kengne, J., Tsafack, N., Kengne, L.K. (2018). Dynamical analysis of a novel single Opamp-based autonomous LC oscillator: antimonotonicity, chaos, and multiple attractors. International Journal of Dynamics and Control, 6(4): 1543-1557. https://doi.org/10.1007/s40435-018-0414-2

[15] Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A.M., Hirota, K., Abd EL-Latif, A.A. (2020). Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Information Sciences, 515: 191-217. https://doi.org/10.1016/j.ins.2019.10.070

[16] Arpacı, B., Kurt, E., Çelik, K., Ciylan, B. (2020). Colored image encryption and decryption with a new algorithm and a Hyperchaotic electrical circuit. Journal of Electrical Engineering & Technology, 15(3): 1413-1429. https://doi.org/10.1007/s42835-020-00393-x

[17] Vaidyanathan, S., Akgul, A., Kacar, S. (2018). A new chaotic jerk system with two quadratic nonlinearities and its applications to electronic circuit implementation and

image encryption. International Journal of Computer Applications in Technology, 58(2): 89-101. https://doi.org/10.1504/IJCAT.2018.094572
[18] Muhammad, A.U.S., Özkaynak, F. (2021). SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs. Symmetry, 13(5): 824. https://doi.org/10.3390/sym13050824
[19] Mokhnache, A., Ziet, L. (2020). Cryptanalysis of a pixel permutation based image encryption technique using chaotic map. Traitement du Signal, 37(1): 95-100. https://doi.org/10.18280/ts.370112
[20] Etem, T., Kaya, T. (2020). A novel true random bit generator design for image encryption. Physica A: Statistical Mechanics and Its Applications, 540: 122750. https://doi.org/10.1016/j.physa.2019.122750
[21] Özkaynak, F. (2020). On the effect of chaotic system in performance characteristics of chaos based s-box designs. Physica A: Statistical Mechanics and its Applications, 550: 124072. https://doi.org/10.1016/j.physa.2019.124072
[22] Trujillo-Toledo, D.A., López-Bonilla, O.R., García-Guerrero, E.E., Tlelo-Cuautle, E., López-Mancilla, D., Guillén-Fernández, O., Inzunza-González, E. (2021). Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. Chaos, Solitons & Fractals, 153: 111506. https://doi.org/10.1016/j.chaos.2021.111506
[23] Patro, K.A.K., Soni, A., Netam, P.K., Acharya, B. (2020). Multiple grayscale image encryption using cross-coupled chaotic maps. Journal of Information Security and Applications, 52: 102470. https://doi.org/10.1016/j.jisa.2020.102470
[24] Campos-Cantón, I., Campos-Cantón, E., Murguía, J.S., Rosu, H.C. (2009). A simple electronic circuit realization of the tent map. Chaos, Solitons & Fractals, 42(1): 12-16. https://doi.org/10.1016/j.chaos.2008.10.037
[25] Zhu, C., Wang, G., Sun, K. (2018). Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box. Symmetry, 10(9): 399. https://doi.org/10.3390/sym10090399
[26] Lu, Q., Zhu, C., Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. IEEE Access, 8: 25664-25678. https://doi.org/10.1109/ACCESS.2020.2970806
[27] Avaroğlu, E. (2017). LFSR soru girdisi ile PUF tasarımının gerçeklenmesi. Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 29(2): 15-21.
[28] Pourasad, Y., Ranjbarzadeh, R., Mardani, A. (2021). A new algorithm for digital image encryption based on chaos theory. Entropy, 23(3): 341. https://doi.org/10.3390/e23030341
[29] Yosunlu, D., Avaroğlu, E. (2021). Son İşlem Algoritmaları İçin Web Tabanlı Yazılım Suiti Geliştirilmesi. Avrupa Bilim ve Teknoloji Dergisi, 2021(28): 493-499. https://doi.org/10.31590/ejosat.1008063
[30] Anandakumar, N.N., Sanadhya, S.K., Hashmi, M.S. (2019). FPGA-based true random number generation using programmable delays in oscillator-rings. IEEE Transactions on Circuits and Systems II: Express Briefs, 67(3): 570-574. https://doi.org/10.1109/TCSII.2019.2919891
[31] Suresh, V.B., Burleson, W.P. (2010). Entropy extraction in metastability-based TRNG. In 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 135-140. https://doi.org/10.1109/HST.2010.5513099
[32] Buscarino, A., Fortuna, L., Frasca, M., Sciuto, G. (2014). A concise guide to chaotic electronic circuits. Heidelberg, Germany: Springer International Publishing. Springer, New York, https://doi.org/10.1007/978-3-319-05900-6
[33] Rukhin, A. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Special Publication 800- 22 Revision 1a.
[34] Xian, Y., Wang, X., Yan, X., Li, Q., Wang, X. (2020). Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion. Optics and Lasers in Engineering, 134: 106202. https://doi.org/10.1016/j.optlaseng.2020.106202
[35] Khan, M., Masood, F. (2019). A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimedia Tools and Applications, 78(18): 26203-26222. https://doi.org/10.1007/s11042-019-07818-4
[36] Wang, X., Xue, W., An, J. (2020). Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of household. Chaos, Solitons & Fractals, 141: 110309. https://doi.org/10.1016/j.chaos.2020.110309