International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6588
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 08 April 2023*

Pseudo Random Binary Sequences Obtained Using Novel Chaos Based Key Stream Generator and their Auto-correlation Properties

Pushpalatha G S[1], Ramesh S[2]
[1]Research Scholar, Department of Electronics & Communication Engineering
Dr. Ambedkar Institute of Technology, Visvesvaraya Technological University
Belagavi, India
e-mail: pushpalathags.ec@drait.edu.in
[2]Professor, Department of Electronics & Communication Engineering
Dr. Ambedkar Institute of Technology, Visvesvaraya Technological University
Belagavi, India
e-mail: rameshs.ec@drait.edu.in

Abstract— In this paper, psuedo random binary sequences are generated from the "Chaos Based Key Stream Generator- using novel Permutation technique with two dimensional patterns and substitution technique with Z_4 mapping" and investigation of auto correlation property for the generated seuwnces is presented. Initially a chaotic function, considering Logistic map is used to generate a Pseudo Random Numbers (PRNs). Then these numbers are converted into binary sequences using binary mapping. These sequences are further modified by novel permutation techniques defined using 2-Dimensional patterns, and substitution technique defined over Z_4 transformation in order to improve their statistical properties. The resulting sequences are investigated for auto correlation properties using Normalized Hamming Auto Correlation function. The purpose of this work is to assessing the quality of sequences of uniformly distributed pseudorandom numbers from the proposed generator. It is found that, generated sequences exhibit good auto-correlation property which is suitable for key sequence or secret key for cryptographic applications.

Keywords- Pseudo Random Numbers (PRN's), Chaos Based Cryptography, Auto Correlation test, Stream Ciphers, Data Security.

I. Introduction

Recent developments in internet technologies has the major concern for data security to maintain confidentiality, integrity, and authenticity. This has led to the various research and developments in cryptography. In addition to the available traditional cryptographic algorithms, designing new algorithms suitable for real time applications is challenging. Alternately, chaos based cryptography is also finding interest due to their randomness properties such as high non-linearity, sensitivity to initial conditions, large periodicity, uniform distribution etc. [1-2].

Random numbers or Pseudo Random Numbers (PRN's) are widely used in various applications like secure communication, gaming industry, software testing, VLSI testing , AI based decision making algorithms etc. in modern technological fields. The required characteristics of PRN's such as unpredictability, periodicity, uniform distribution property, correlation, ergodicity etc. depends on the applications [3-7]. Sequences having better randomness properties are desirable for cryptographic applications and are widely used as secret key for symmetric key system.

In recent decade chaos based random number generators are emerging as alternate methods for traditional algorithms due to their highly nonlinear nature. Chaos based cryptography offers better cryptographic needs with respect to key generation. The first attempt of using the chaos theory in cryptography was initiated by Robert Matthews in 1989 through his work, which attracted much interest [8]. Chaotic maps-based cryptographic model includes various one-dimensional chaotic maps like logistic, cubic, tent and quadratic map etc. While designing chaos-based cryptographic algorithms, the practical problem arises due to difficulty in achieving high precision. Chaotic functions are of important classes of random sequence generation for stream cipher system [9-10]. Some of the stream cipher algorithms based on chaotic systems and their implementations are discussed in [11-15].

One of the important components of Pseudo Random Numbers (PRN's) is family of sequences having good correlation properties for sequence length over suitable length. Use of sequence having better autocorrelation function is suitable for cryptographic applications. The good correlation property for Pseudo Random Numbers (PRN's) is usually measured using autocorrelation function. Hamming

Autocorrelation function may be used to find the correlation function of random binary sequence [16-22]. Autocorrelation is a statistical test that determines whether a random number generator is producing independent random numbers in a sequence. The autocorrelation tests are concerned with the degree of correlation of numbers in a sequence.

II. Proposed Model of Chaos Based Key Stream Generator (CBKSG) Using Novel Permutation and Substitution Techniques

The proposed method uses a novel permutation and substitution techniques for generating pseudo random binary sequence. The process involved in the proposed model to generate pseudo random binary sequence from the proposed 'Chaos-Based Key Stream Generator (CBKSG)' using novel permutation and substitution techniques is as shown in "Fig. 1".

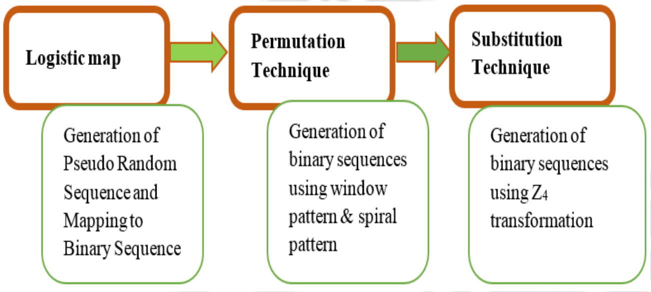

Logistic map
Permutation Technique
Substitution Technique
Generation of Pseudo Random Sequence and Mapping to Binary Sequence
Generation of binary sequences using window pattern & spiral pattern
Generation of binary sequences using Z4 transformation

Figure 1. Proposed Chaos-Based Key Stream Generator (CBKSG)

The process is briefly explained as follows. Initially Pseudo Random Numbers (PRNs) are generated using logistic map. Then novel permutation and substitution techniques are applied to the resultant sequences of logistic map. A novel permutation technique is defined by various two-dimensional patterns and substitution technique is defined by Z_4 mapping.

In permutation technique, the defined patterns are named as window pattern and spiral pattern. They are made to visit randomly on the resultant binary sequence of logistic map which are arranged in two-dimensional space. The random visit made by the 2-Dimensional patterns are considered to construct new binary sequences and they are tested for their auto correlation properties. In substitution technique, binary sequences obtained after the permutation are subjected to nonlinear mapping Z_4 transformation to obtain new binary sequences and they are tested for their auto correlation properties. The process for generating pseudo random binary sequence involves three stages. In stage-1, logistic map is used to generate pseudo random sequences. In stage-2, a novel permutation technique is developed and applied. In stage-3, a novel substitution technique is developed and applied. They are briefly explained in the following section.

A. Stage-1: Logistic map

In first stage, a pseudo random sequence (floating in nature) is generated using a logistic map as defined in (1). The bifurcation diagram of Logistic map is as shown in "Fig. 2".

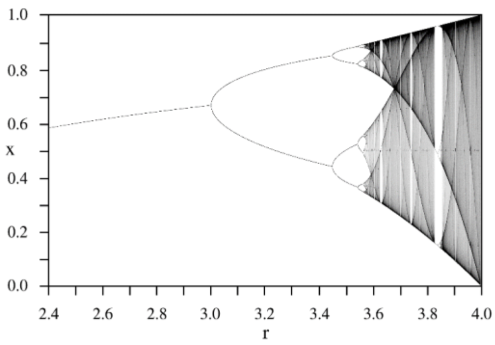


Figure 2. Bifurcation diagram of Logistic Map

It exhibits the chaotic behavior in the range 3.99≤ r < 4. The output of logistic map is a floating point sequences which is considered in the range of 0.000000 to 0.999999 and mapped to integer of six digits. Then it is converted into a binary stream of length N=10^6.

$$x_{n+1} = r x_n (1 - x_n) \tag{1}$$

Where $0 \le x_0 < 1$ and $0 \le r < 4$;

x_0 *the initial value* , x_{n+1}, the next value

Example 1: If the number obtained from logistic map is 0.125536 (floating point), then it is converted to a integer number (I_n) by multiplying 10^6, which results in 125536 , this number will then be converted into binary number '1' by using (2).

$$B = \begin{cases} 1, & I_n = Even \\ 0, & I_n = Odd \end{cases} \tag{2}$$

The binary sequence {B} obtained from this stage will undergo permutation process by novel permutation techniques which are explained in next section.

B. Permutation Technique

In second stage, two dimensional permutation patterns called 'Window Pattern' is denoted by '$\mathbf{P_w}$' and 'Spiral Pattern' is denoted by '$\mathbf{P_s}$' are defined as shown in "Fig. 3" and "Fig. 4" respectively. In $\mathbf{P_w}$, the nodes $*_{()}$ and $O_{()}$ represents the path of binary numbers which have to be traced as per the order of window pattern 1 to 9 which is defined over 3×3 matrix. In $\mathbf{P_s}$, the binary values have to be traced as per the spiral pattern with the initial position considered as {N/2, N/2} for any square matrix of size N.

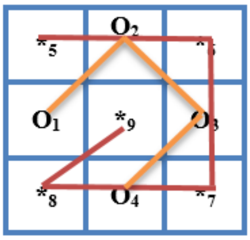


Figure 3. Window pattern

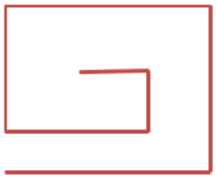


Figure 4. Spiral pattern

The window pattern is considered as the first permutation technique which is applied to the resultant binary numbers of logistic map from stage-1 which are arranged in large two dimensional space. The spiral pattern is considered as the second permutation technique which is applied to the resultant binary numbers from window pattern which are arranged in large two dimensional space. Then, the binary sequences obtained from this stage will undergo substitution process which is considered as stage-3.

C. *Stage-3: Substitution Technique*

Define In third stage, substitution process called Z_4 mapping is defined and applied to the output sequences of stage-2. The Z_4 mapping process is explained as follows.

- Sequence over $\{Z_4\}$ is defined as $\{Z_4\}= \{ 0,1,2,3\}$
- Binary 2-tuple of binary sequences (B_2) which are obtained from stage-2 are mapped to Z_4 elements as depicted in “Fig. 5”.

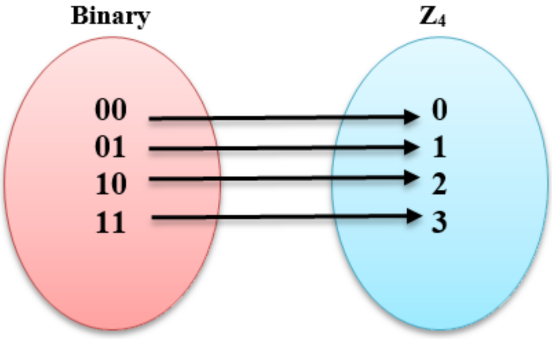


Figure 5. Binary to Z_4 mapping

Final binary sequence ‘B’, is obtained by mapping the Z_4 sequence back to binary as defined in (3) and depicted in “Fig. 6”. The overall process is explained with an illustration for each stage in the following section.

$$\mathrm{B} = \begin{cases} 1, & For\ 0,3 \in \mathrm{Z4} \\ 0, & For\ 1,2 \in \mathrm{Z4} \end{cases} \qquad (3)$$

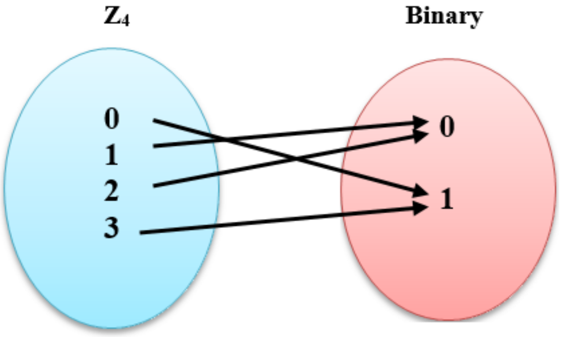


Figure 6. Z_4 to Binary mapping

D. *Illustration*

a) Stage-1: Logistic map

Let us consider a 36 bit binary sequence (B_s) resulted from logistic map is given in (4). B_s is arranged in a 2-D Matrix of size 6×6 as shown in “Fig. 7”, which is then shuffled in next stage by using permutation patterns.

$$B_S = \{011010100101101101001101100110011010\} \quad (4)$$

0	1	1	0	1	0
1	0	0	1	0	1
1	0	1	1	0	1
0	0	1	1	0	1
1	0	0	1	1	0
0	1	1	0	1	0

Figure 7. Binary sequence obtained from logistic map

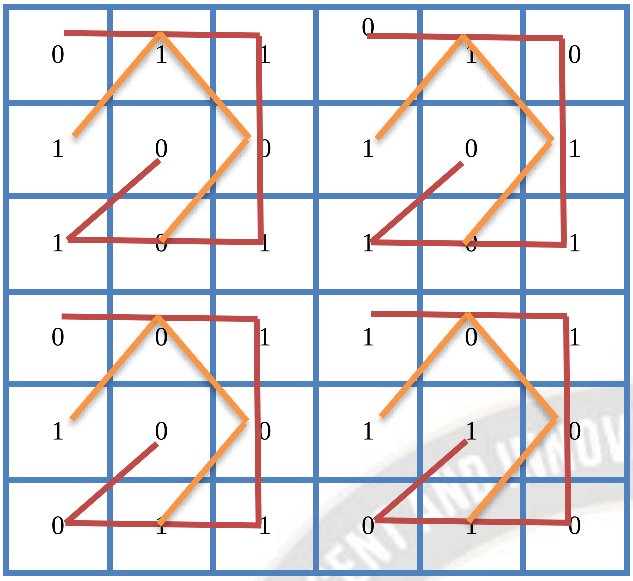
E. *Stage-2: Permutation Technique*

a) Window pattern

A window pattern will be applied for the binary values which are arranged in 2-D space as shown in “Fig. 8”. The pattern will be moved from left to right along the binary values from the top left position to bottom right position without overlapping. The trace for each window is as discussed in the section 2.2. The permuted binary sequence is generated as per the path traced by the window pattern (as shown in figure.3) is given by B_1 in (5).

$$B_1 = \{110001110111000110100101100100111001\} \quad (5)$$

***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 08 April 2023*



0	1	1	0	1	0
1	0	0	1	0	1
1	0	1	1	0	1
0	0	1	1	0	1
1	0	0	1	1	0
0	1	1	0	1	0

Figure 8. Application of a window pattern

The sequence B_1 is then arranged in a 2-D Matrix of size 6×6 as shown in "Fig. 9".

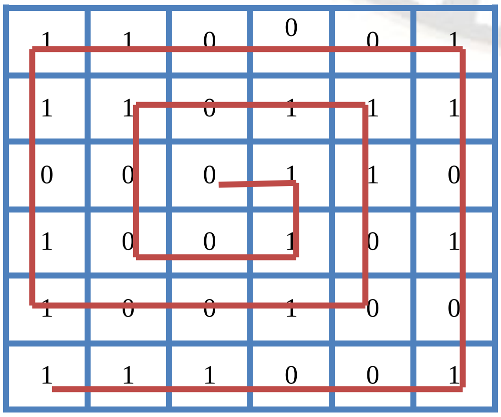
1	1	0	0	0	1
1	1	0	1	1	1
0	0	0	1	1	0
1	0	0	1	0	1
1	0	0	1	0	0
1	1	1	0	0	1

Figure 9. Permuted sequences from window pattern

b) Spiral pattern

A spiral pattern will be applied as shown in "Fig .10" for the binary values resulted from the window pattern shown in "Fig. 9". Permuted binary sequence is generated as per the path traced by the spiral pattern is given by B_2 in (6).

$B_2 = \{011000101110010011011100011010100111\}$ (6)



1	1	0	0	0	1
1	1	0	1	1	1
0	0	0	1	1	0
1	0	0	1	0	1
1	0	0	1	0	0
1	1	1	0	0	1

Figure 10. Application of a spiral pattern

F. Stage-3: Substitution Technique

Substitution technique, Z_4 mapping is applied to the output sequences of stage-2 as illustrated below. The resultant final binary sequence is denoted as B in (7).
Consider the sequence

B_2={011000101110010011011100011010100111} and

Corresponding {Z_4} sequence = {120232………..}

Mapped final binary sequence 'B' is given in (7).

$$B = \{100010 \dots \dots \dots\} \qquad (7)$$

In this manner a set of about 10000 binary sequences each of length 10^6 are generated for various initial values 'x_0' and system parameter 'r'. These sequences will be further tested for auto correlation properties.

III. Normalized Cyclic Hamming Autocorrelation (NCHA) Function

Autocorrelation plots are generally used to know whether the sequence possess randomness properties. This randomness is determined by computing autocorrelation for sequences. If the value of autocorrelation of sequence is very small or negligible for all shifts of the sequences, such sequences are considered to be random and for non-random sequences such value will be significantly higher for more shifts.
Normalized Cyclic Hamming Autocorrelation function is defined in the following section, and it is used to determine the randomness of the sequence generated using the proposed method.

A. Definition and Illustration

The normalized cyclic Hamming auto correlation function of two binary sequences {S} and its shifted version {S'} of length N is defined in (8a) and (8b) followed by (8).

$$\alpha_{SS'}(\tau) = [N_a - N_d] \,/\, \mathrm{N}, \quad 0 \le \tau \le \mathrm{N} - 1 \qquad (8)$$

Where,
$\alpha_{ss'}(\tau)$ is the normalized cyclic Hamming auto correlation function of binary sequence S and its shifted versions S′
N=Length of the sequence
N_a=Number of agreements of symbols
N_d =Number of dis-agreements of symbols between the sequence S and its circularly shifted version S′ and,
τ = Shift parameter

This is illustrated as follows
Consider the binary sequence S of length 20 bits as in (8a).

$S = \{101000110\ 01111000111\}$ (8a)

It's circularly shifted to right by one bit position ($\tau = 1$) represented as S' and is given in (8b).

$S' = \{1101000110\ 0111100011\}$ (8b)

The number of agreements and number of disagreements for the example sequences S and S′ is listed in table (1). It is found that the number of agreements and disagreements between sequence S and S′ is N_a=11 and N_d=09 respectively. Computing $\alpha_{ss'}(1) = (N_a - N_d) / N$, we get the value as 0.1. Similarly $\alpha_{SS'}(\tau)$ value may be obtained for all the shifts (τ) [0 to N-1].

TABLE 1: Number of agreements and number of disagreements for the example sequences S and *S′*

S	1	0	1	0	0	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1
S′	1	1	0	1	0	0	0	1	1	0	0	1	1	1	1	0	0	0	1	1
a / d	a	d	d	d	a	a	d	a	d	d	d	a	a	a	d	a	a	d	a	a

B. Case studies

The value of $\alpha_{ss'}(\tau)$ is computed by considering various cases of binary sequences generated using the proposed method to study the correlation properties of the sequences shown in table 2. The plots of autocorrelation tests are shown in "Fig.11" and "Fig.12" for different cases.

- **Case 1**

In this case the initial value x_0 is varied and system parameter 'r' value is maintained constant as per (1), to generate the binary sequences using the proposed method, the resultant sequences are subjected to autocorrelation test.

For example, for variable initial value say x_0=0.091921 and fixed parameter r = 3.9, sequences can be obtained by varying x_0. The corresponding NCHA plots are as shown in "Fig. 11".

- **Case 2**

In this case the initial value x_0 is maintained constant and system parameter 'r' value is varied as per (1), to generate the binary sequences using the proposed method, the resultant sequences are subjected to autocorrelation test.

For example, for fixed x_0=0.091921 and variable parameter r = 3.911, sequences can be obtained by varying 'r'. The corresponding NCHA plots are as shown in "Fig. 12".

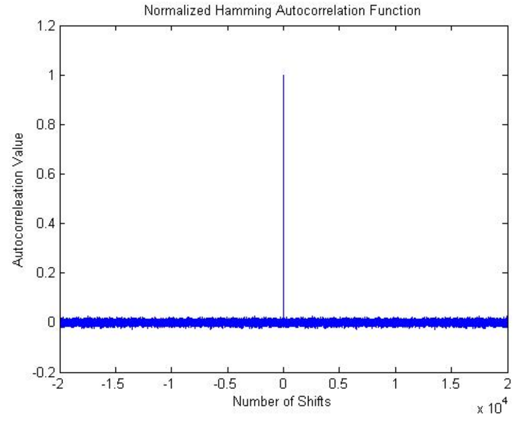
It is evident from NCHA plots that the off peak value is small and ranges are almost in the vicinity of -0.001 to +0.03. This shows the autocorrelation value is very small for all the shifted versions of the sequences, except the peak value at the origin. This indicates that the random nature of the sequence is obtained from the proposed method.

In this way, a set of 10000 sequences are generated and tested for auto correlation properties. Majority of the sequences pass auto-correlation tests. Thus the sequences are found to be pseudo random in nature as suitable for cryptographic applications.

TABLE 2: Auto-correlation test results

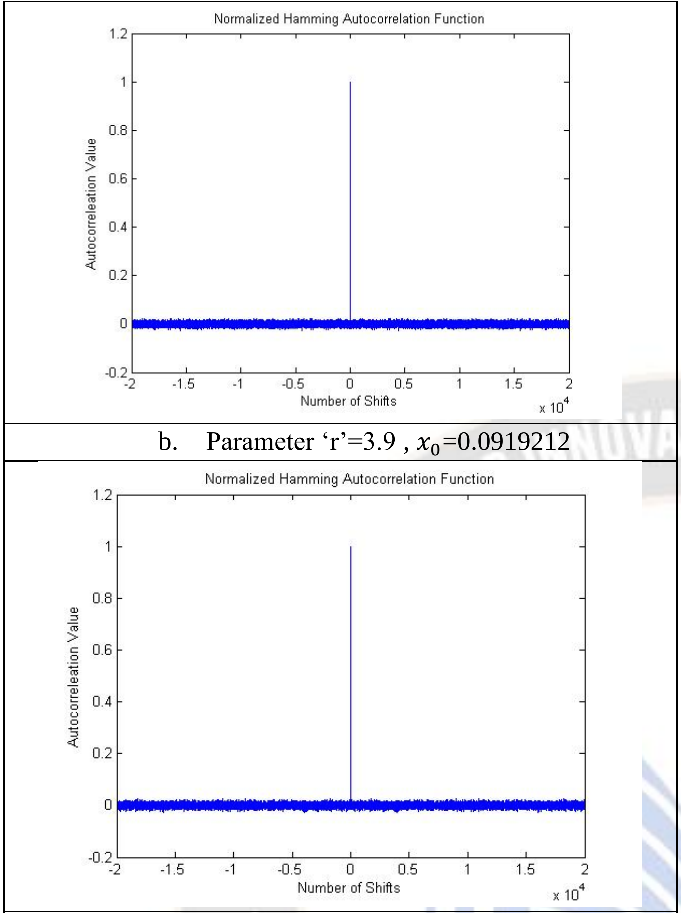
Case Study: Map used: Logistic map Length of sequence =20000 bits	Initial values of the proposed PRNG		Range of autocorrelation value (approximate)	Implication
Case 1	r=3.9	x_0=0.091921	-0.001 to +0.03	Pass
		x_0=0.0919212	-0.001 to +0.03	Pass
		x_0=0.0919213	-0.001 to +0.03	Pass
Case 2	x_0 =0.091921	r=3.911	-0.001 to +0.03	Pass
		r=3.912	-0.001 to +0.03	Pass
		r=3.913	-0.001 to +0.03	Pass

Case 1: Map used: Logistic map
Length of sequence =20000 bits
'r' fixed, 'x_0' varied



a. Parameter 'r'=3.9 , x_0=0.091921

DOI: https://doi.org/10.17762/ijritcc.v11i5.6588
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 08 April 2023*

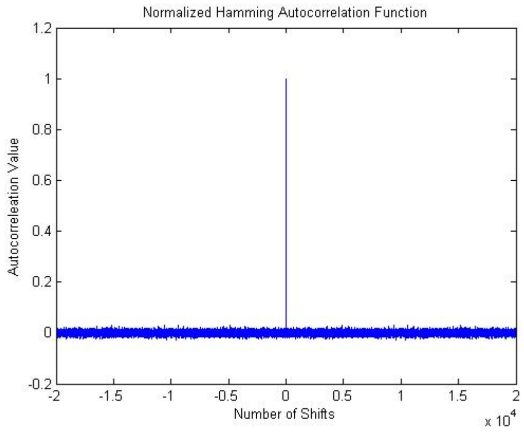


b. Parameter ‘r’=3.9 , x_0=0.0919212

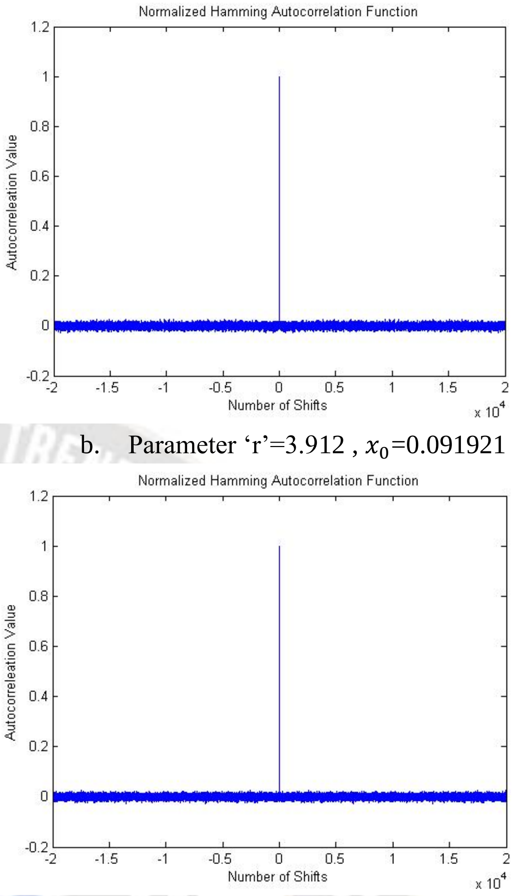
c. Parameter ‘r’=3.9 , x_0=0.0919213

Figure 11. NCHA Plot of binary sequences obtained at final stage

Case 2: Map used: Logistic map
Length of sequence =20000 bits
‘x_0’ fixed, ‘r’ is varied



a. Parameter ‘r’=3.911 , x_0=0.091921



b. Parameter ‘r’=3.912 , x_0=0.091921

c. Parameter ‘r’=3.913 , x_0=0.091921

Figure 12. NCHA Plot of binary sequences obtained at final stage

CONCLUSION

In this work, the pseudo random binary sequences are generated by the proposed model “Chaos Based Key Stream Generator” which uses novel permutation and substitution techniques and an auto correlation test is carried out on the resultant sequences by considering various parameters like initial value (x_0) and system parameter function (r). From the results it is seen that majority of the sequences exhibit good auto correlation properties as in the previous cases discussed. Hence it if evident that probability of randomly chosen sequences exhibit better autocorrelation properties which is desirable for the random sequence for consideration for cryptographic application for encryption of message. Thus, the binary sequences generated from proposed model using novel permutation technique with various two dimensional patterns and substitution technique with Z4 mapping proves to be an efficient ‘Pseudo Random Binary Sequences’ as suitable for cryptographic applications.

ACKNOWLEDGMENT

This research work is funded by Vision Group of Science and Technology (VGST), Govt. of Karnataka (GRD 575). The authors acknowledge the support for the research work by VGST. The authors would also like to thank Dr. Ambedkar Institute of Technology, Bengaluru for providing the research support.

REFERENCES

[1] Alfred J Menezes, Paul C. Van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, New York, 1997.

[2] William Stallings, “Cryptography and Network Security”, Principles and Practice, 5th Edition, Pearson Education Inc, 2006.

[3] Francois Panneton and Pierre L’Ecuyer, “Random Number Generators Based on Linear Recurrences in”, Monte Carlo and Quasi-Monte Carlo Methods, Niederreiter H., Editor, Springer-Verlag, 2004, pp.367-378, 2002.

[4] Francois Panneton and Pierre L’Ecuyer, “On the Xorshift Random Number Generators", ACM Transactions on Modeling and Computer Simulation, 15, 4, pp 346-361, 2005.

[5] Francois Panneton, Pierre L'Ecuyer, Makoto Matsumoto , “Improved Long-period Generators Based on Linear Recurrences Modulo 2”, ACM Trans. Math. Software. 32(1): pp.1-16. 2006.

[6] Bernstein G. M. and Lieberman M. A., “Secure Random Number Generation Using Chaotic Circuits”, IEEE Trans. Circuits Syst., Vol. 37, No. 9, pp. 1157-1164, 1990.

[7] Claude Shannon, “Communication Theory of Secrecy Systems”, Bell System Technical Journal, 28 (4), pp 656–715, 1949.

[8] R. Matthews, “On the derivation of a chaotic encryption algorithm”, Cryptologia, XIII (1), pp 29–42, 1989.

[9] Madhekar Suneel, “Cryptographic Pseudo-random Sequences from the Chaotic Henon Map”, Sadhana, Indian Academy of Sciences, Vol. 34, Part 5 , pp. 689–701, 2009.

[10] Vinod yt Patidar and Sud K. K., “A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing”, Informatica 33, pp. 441–452, 2009.

[11] Kitsos p., D. Gligoroski et al, “On the Hardware Implementation of the Mickey-128 Stream Cipher”, Cryptology ePrint Archive, Report, Presented in the eSTREAM publications List, pp 301, 2005.

[12] Kitsos P., Kaiser U., “A high-speed Hardware Implementation of the Hermes 8-128 Stream Cipher”, European Conference on Circuit theory and Design-Seville, pp. 364-367, 2008.

[13] Li Shujun, Mou Xuanqin, Cai Yuanlong, “Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher”, Indocrypt,LNCS, 2001.

[14] P. Kitsos and A. N. Skodras, “On the Hardware Implementation of the MUGI Pseudorandom Number Generator”, In proceedings of the Fifth International Symposium on Communications Systems, Networks and Digital Signal Processing, Patras, Greece, 2006.

[15] Kitsos P., G. Kostopoulos, Sklavos N., and Koufopavlou O. , "Hardware Implementation of the RC4 Stream Cipher”, 46th IEEE Midwest Symposium on Circuits & Systems, Cairo, Egypt, pp. 27-30,2003.

[16] Matt J. B. Robshaw, “Stream Ciphers Technical Report-TR-701”, Version 2.0 (RSA Laboratories), 1995.

[17] Goresky M. and Klapper A, “Algebraic Shift Register Sequences”, Cambridge university press, pp. 230-249, 2012.

[18] Soloman Wolf Golomb, “Shift Register Sequences”, San Francisco:Holden Day, Reprint Aegan Park Press, Laguna Hills, California,1967.

[19] Dieter Gollmann and William G. Chambers, “Clock-Controlled Shift Registers: a Review”, IEEE Journal on Selected Areas in Communications, 7(4), pp. 525–533, 1989.

[20] Ekdahl P and Johansson T, SNOW-A New Version of the Stream Cipher SNOW, Selected Areas in Cryptography, (Springer-Verlag), LNCS 2595, pp. 47-61, 2003.

[21] Soloman Wolf Golomb and Guang Gong, “Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar”, Cambridge University Press, 2005.

[22] Ramesh, S; Murali, R; Haribhat, KN, “Generation of Sequence of Random Numbers defined over Z_4 and their correlation properties”, International Conference on Communication Technology. IEEE, pp 1-4, 2006.