International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 24 (2018) pp. 16945-16949

Binary Sequences in Chaotic systems: A Review

K. Chidananda Murthy [1], Mahalinga.V. Mandi [2], R. Murali[3]
[1] *Research Scholar, Department of Electronics and Communication Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, India.*

[2] *Professor, Department of Electronics and Communication Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, India.*

[3] *Professor, Department of Mathematics, Dr. Ambedkar Institute of Technology, Bengaluru, India.*

Abstract:

Chaotic systems have a number of interesting properties such as sensitivity on initial condition and system parameter, ergodicity and mixing (stretching and folding) properties, etc. These properties make the chaotic systems a worthy choice for constructing the cryptosystems as sensitivity to the initial condition/system parameter and mixing properties respectively are analogous to the confusion and diffusion properties of a good cryptosystem. In this paper we present a review of chaotic binary sequences using different chaotic maps like Logistic map, Tent map, Cubic map and coupled chaotic map and their suitability in cryptographic application systems.

Keywords: Chaotic maps, chaotic functions, spread spectrum communication, Code division multiple access.

1. INTRODUCTION

Chaos is characterized by deterministic nonlinear nonperiodic nonconverging and bounded behaviour. Chaotic sequence is an example of a discrete time continuous amplitude random sequence. The main characteristic of chaotic sequences is its sensitive dependence on initial conditions. Even if a small difference is introduced between the initial values, two chaotic sequences separate typically from each other after a short time period and are highly uncorrelated. Therefore, by using different initial values it is possible to produce a large number of chaotic sequences. One of the well-known one dimensional iterative maps which exhibits chaotic properties is logistic map which is regarded as a first order nonlinear recurrence equation over a real field.

Chaotic systems have a number of interesting properties such as sensitivity on initial condition and system parameter, ergodicity and mixing (stretching and folding) properties, etc. These properties make the chaotic systems a worthy choice for constructing the cryptosystems as sensitivity to the initial condition/system parameter and mixing properties respectively, are analogous to the confusion and diffusion properties of a good cryptosystem. In this article we present a review of chaotic binary sequences which possess the desirable properties for cryptographic applications. Some of the cryptographic applications in real time can be found in [1] to [10].

2. LITERATURE SURVEY

In this section we present a review of chaotic binary sequences in cryptographic applications and CDMA.

In [11], Narendra et.al. have discussed the concept of a random bit generator using chaotic maps. In this paper, the authors have proposed a new binary sequence generator called cross-coupled chaotic random bit generator (CCCBG) which exploits the interesting properties of a skew tent map. In the proposed CCCBG, authors have chosen two skew tent maps which are piecewise linear chaotic maps and cross-coupled. Using cross coupling, the authors show a forceful change in the behavior of both the chaotic maps regularly. By knowing the system parameter and initial conditions of one of chaotic maps, the behavior of CCCBG can be easily identified. The authors have used four statistical tests namely frequency test, Poker test, auto-correlation test and serial test on several large sized binary sequences generated by CCCBG to evaluate randomness and uniformity. The authors have also used NIST suite tests to evaluate the randomness of the bit streams generated by CCCBG.

In [12], Sukalyan Som et.al. have discussed RGB image encryption algorithm based on DNA coding and a chaos based pseudo random binary number generator. In this paper the authors have proposed an algorithm by scrambling the plain image using a generalized Arnold cat map in order to increase security. The scrambled image pixel is converted to DNA codes and again reconverted to integers where the choice of DNA coding rule is made pseudo random by the binary stream generated by chaos based PRBNG. The integers obtained after DNA coding and re-coding are diffused by performing exclusive OR operation with the integer sequences generated by 1D Logistic map producing the cipher image. The experimental results suggest that the proposed algorithm can successfully encrypt and decrypt RGB color images with secret keys. The simulation analysis shows that the proposed method is loss-less, secure and efficient. The authors have performed statistical tests like histogram analysis, correlation coefficient analysis, measures of central tendency and dispersion to authenticate their results.

In [13], Mahalinga V.Mandi et.al. have presented a new method of generation of chaotic discrete and binary sequences using Logistic map, Tent map and Cubic map. Normally in these schemes, cross correlation has a minimum value but not zero. If the number of users increases at a time, there is degradation in the quality of the received

signal. The generated discrete and binary sequences are analyzed for autocorrelation and cross correlation properties and those sequences having desirable properties can be used for CDMA application.

Chikhaoui Fatima et.al. in [14] have discussed new chaotic binary sequences with good correlation property using logistic maps. In this paper the authors have proposed a new scheme for generating binary sequences from logistic maps. New methods by using several binary sequences with the same length which can be generated directly by assuming different initial conditions to logistic maps and a comparison between conventional sequences (maximum length sequences, Gold sequences) and the proposed sequences has been specified. The sequences generated with proposed schemes have the same length (length is independent of initial conditions) for all initial conditions. Chaotic binary sequences outperform conventional sequences in several key aspects like complexity of generation, flexibility in choosing the length of sequence and multiple access capability.

In [15], Deb Sunder Swami et.al. have discussed logistic map based PN sequence generator for DSSS modulation system. The authors have proposed a PN sequence generator based on one dimensional chaotic logistic map. The generated sequence is used as a spreading sequence in a direct-sequence spread-spectrum modulation scheme in a multipath environment with AWGN and Rayleigh fading channels. The BER curves are obtained and compared with the existing LFSR-based PN sequence generator and Kasami sequence. The comparative study shows that the proposed generator performs better than both. The authors have tested under various channel fading conditions for the generated sequence. Their respective BER curves and channel impulse responses are generated and upon comparison with theoretical standards, the sequence was found to perform under expected lines. Also, a comparative study has been done between logistic map based PN sequence, LFSR based PN sequence and Kasami sequence under slow and fast fading conditions. The BER curves obtained showed that the logistic map based PN sequence performed better than both the other sequences. This means that the PN sequence generated has good cryptographic strength and can be applied for Direct Sequence Spread Spectrum (DSSS) Modulation.

In [16], Ahmad Beirami et.al. have discussed the fundamental performance limits of chaotic-map random number generators. The authors have defined a chaotic map for random number generator (RNG) and a bit generation function. When the map function is exactly known, for a given bit generation function, the entropy-rate of the generated output bit sequence is asymptotically the highest rate at which truly random bits can be generated from the map. The supremum of the entropy-rate amongst all bit-generation functions is called the binary metric entropy, which is the highest rate at which information can be extracted from any given map using the optimal bit-generation function. In this article, the authors provide converse and achievable bounds on the binary metric entropy. The achievability is based on a sequence of universal bit-generation functions in the sense that the bit-generation function is not dependent on the specific map. The proposed sequence of bit-generation functions offers a fairly simple implementation which can easily be realized on hardware for practical purposes.

In [17] the authors Bozhen Cai et.al. have introduced a new chaotic system and have generated a pseudo random sequence from this system. Their work presents a novel chaotic system with a single nonlinear exponential term d^{z^2}. The base d of the exponential term induces a rather complex chaotic system very different from the existing exponential chaotic systems. Theoretical studies and numerical simulations by the authors show that the chaotic signal is extremely complex by the Lyapunov exponent spectrum and bifurcation diagrams. In particular, the bifurcation diagrams suggest inverse period doubling bifurcation and period-four window in the chaotic system. Statistical properties of the chaotic sequences when tested using NIST software suggest that the chaotic system can possess better performances of the well-known Lorenz system. The authors conclude that the proposed chaotic pseudo random sequence can be used for secure communications, data encryption, image processing and other related fields.

Wimol San-Um et.al. have given a cost effective true random bit generator using a pair of robust signum-based chaotic maps in [18]. This system provides a robust chaos against parameter changes and a symmetric bifurcation for zero thresholding for digital random bit generation. Dynamics are described in terms of equilibria and Jacobian analysis, bifurcation diagram, Lyapunov exponent, time-and frequency domain signal and cobweb plots. NIST standard tests suite have been realized for statistical analysis of randomness of binary sequence. The sufficient length of 1,000,000 bits successfully passed all NIST standard tests. Experimental results of digital random-bit sequences have been performed using a cost effective Arduino with Atmel SAM3X8E ARM Cortex-M3 CPU by the authors. Cryptography has extensively been utilized for information security where a True-Random-Bit (TRB) generator is a crucial system not only in confidential key generation, but also in some computation algorithms. Conventional techniques are based on stochastic phenomena and relatively expensive such as random physical phenomenon such as the amplification of direct resistor noises. Chaos dynamics of the signum-baed system have been described in terms of equilibria and Jacobian analysis, bifurcation diagram, Lyapunov exponent, time-and frequency domain signals and cobweb plots. The authors conclude that the proposed random-bit generator offers a potential alternative in compact and robust random bit sequence for applications in computer information security.

Periods of sequences generated by the logistic map over finite fields with control parameter four is studied by Kazuyoshi Tsucidya and Yasuyuki Nogamitt in [19]. If the logistic map is implemented by using finite precision computer arithmetic, rounding is required. In order to avoid rounding, the implementation of logistic map over finite fields is studied. In this paper, the authors show some properties of periods of sequences generated by the logistic map over finite fields with control parameter four. They show conditions for parameters and initial values (given by values of the Legendre symbol) to have a long period and asymptotic properties for periods by

numerical experiments. The authors show the conditions of parameters for maximal sequences on the sets of initial values and estimate a ratio of maximal primes, the number of periods and period lengths on the sets of initial values.

Dimo Malchev and Ilhan Ibryam have studied the construction of pseudorandom binary sequences using chaotic maps in [20]. In this paper, the authors have proposed a modified construction of pseudorandom binary sequences using chaotic maps. Statistical testing of the output binary digits has been done with NIST, DIEHARD and ENT packages and the experimental results show that the output streams possess statistically identical properties with true random values.

Ajinkya et.al. in [21] have studied FPGA implementation of direct sequence spread spectrum transmitter with pseudo chaotic generator. In this paper, the lengths of chaotic sequences are not restricted like LFSR sequences. The generated pseudo-chaotic sequences are investigated for autocorrelation, cross-correlation and balance properties. A method of generating chaotic sequences suitable for use in DS/SS system is described in this paper.

Pseudorandom bit generators based on non-stationary logistic maps is explored by the authors Linfeng Liu et.al. in [22]. Pseudorandom binary sequences play a significant role in many fields such as error control coding, spread spectrum communications and cryptography. Most of the researches on non-stationary models are focused on two kinds of particular models, one is piecewise stationary model and the other is hidden Markov model. For a general case, the only method is to change the non-stationary sequence into stationary one. Three methods are widely used to do this work namely: remove the trends of the state sequences, do differential to the state sequence and use linear combination of two or more non-stationary sequences. The authors present a numerical analysis of their work in this paper which shows that the generated binary sequences have good pseudorandom characteristics and are highly capable to withstand attacks. They conclude that their PRBG is suitable especially in the field of cryptography.

The generation of phase coded pulses using generalized logistic maps was studied by K. Babulu and B.T. Krishna in [23]. In this paper, the authors have presented a method to apply the fractionalization to well-known logistic maps. Bi-phase sequences are generated using conventional logistic maps, fractional order logistic maps. Variation of the merit factor are plotted for various values of fractional orders and initial values and it was observed that as the value of fractional order α increases the merit factor value is also increased. The authors also conclude that bi-phase sequences with high merit factor values can be obtained by suitably selecting the fractional order α.

A method of Generating Pseudorandom Binary Sequences based on 3D Chaotic mapping was studied by B. Liu and Q. Chen in [24]. In this paper, the authors have proposed a new method of generating pseudorandom binary sequences based on 3D chaotic mapping based on the fact that most pseudo-random binary sequence generation methods can not satisfy Golomb's randomness hypothesis. The methodology followed by the authors was: first, three discrete random sequences are generated by the chaotic system, and then choose small sequence numbers in the three sequences to make a new sequence, which will be transformed into binary sequence. The authors through a large number of repeated tests observed that every longer sequence in the generated binary ones can pass the frequency test and sequence test, and the correlation and random tests also reach a satisfactory result.

A Low-Cost True Random Bits Generator Based on Chaotic system and light nature was proposed by Alaa. K.F and Hakeem. I.M in [25]. The authors claim that this is a simple and low cost TRNG whose is convenient and compact. The randomness of this physical generator is guaranteed by the characteristics of chaos theory and the intrinsic random nature of the light. By retaining a 1-LSB, the final output binary sequences were found to be highly randomized. The statistical and theoretical analysis proved that the final outputs were truly random and can be used specialized applications

The role of improved logistic map in image encryption was analysed by Mohamed et.al. in [26]. Their study focuses on improving the logistic map which, according to the authors, results in a better and complex chaotic map that provides higher efficacy in encryption than the existing logistic map. The design of the improved logistic map is in such a way to intake one initial and two control parameters and to behave chaotically. The sternness of the proposed algorithm was validated through key space, histogram, correlation coefficient, Net Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), entropy and NIST randomness analyses. The experimental metrics were compared with the available literature. The authors observed that the improved logistic map yields higher bifurcation range which can resist brute force attack. Other experimental metrics proved that the proposed cryptosystem was secured markedly against various statistical, differential and entropy attacks.

3. CONCLUSION

In this paper, we present a review of chaotic binary sequences and their applications in cryptographic applications are discussed. We find that either the generation method is complex or the period of the sequence is limited and in most of the cases, chaotic binary sequences are not applied with NIST test suite to test randomness properties. Hence, design and development of a new chaotic binary sequence generator based on logistic map which produces cryptographically secure pseudo random bit sequences is very essential in future work.

REFERENCES

[1] George Makris, Ioannis Antoniou, “Cryptography with Chaos”, Proceedings, 5th Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens, Greece.

[2] Adriana VLAD, Adrian LUCA, Octavian HODEA, Relu TATARU, “Generating Chaotic Secure

Sequences Using Tent Map And A Running-Key Approach", Proceedings Of The Romanian Academy, Series A, Volume 14, Special Issue 2013, pp. 295–302.

[3] Vinod Patidar, K. K. Sud and N. K. Pareek, 2009, "A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing", Informatica 33, pp. 441–452, .

[4] Jonathan M Blackledge, 2008, "Multi-algorithmic Cryptography using Deterministic Chaos with Applications to Mobile Communications", ISAST Transactions On Electronics And Signal Processing, Vol. 1, No. 2, pp. 234-246..

[5] S. C. Phatak and S. Suresh Rao, "Logistic Map: A Possible Random Number Generator", rXiv: cond-mat/9310004v1 1 Oct 1993.

[6] FatihOzkaynak, SırmaYavuz, 2013, "Security problems for a pseudorandom sequence generator based on the Chen Chaotic system", Computer Physics Communications 184, pp. 2178–2181.

[7] Vinod Patidar and K. K. Sud, 2009, "A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing", Electronic Journal of Theoretical Physics 6, No. 20, pp.327–344.

[8] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, 2013, "Text Encryption Scheme Realized with a Chaotic Pseudo-Random Bit Generator", Journal of Engineering Science and Technology Review 6 (4), pp.9-14.

[9] Ankur A. Khare, Piyush B. Shukla and Sanjay C. Silakari, 2014, "Secure and Fast Chaos based Encryption System using Digital Logic Circuit", I.J. Computer Network and Information Security, 6, pp. 25-33.

[10] Nitin Kumar, Deepika, DivyaWadhwa, Deepak Tomer and S. Vijayalakshmi, 2014, "Review on Different Chaotic Based Image Encryption Techniques", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 2, pp. 197-206.

[11] Narendra K Pareek, Vinod Patidar, and Krishan K Sud, 2010, "A Random Bit Generator Using Chaotic Maps", International Journal of Network Security, Vol.10, No.1, pp.32-38,.

[12] Sukalyan Som, Atanu Kotal, Ayantika Chatterjee."A Colour Image Encryption Based On DNA Coding and Chaotic Sequences", International Conference on Emerging Trends and Applications in Computer Science (ICETACS), 13th - 14th Sept 2013, pp. 108 – 114.

[13] Mahalinga V. Mandi, K. N. Haribhat, R Murali, "Deriving Binary Sequences from Chaotic Sequences having Good Cross Correlation Properties", IEEE International Conference on Machine Intelligence Research and Advancement (ICMIRA), IEEE Computer Society, 21st – 23rd Dec' 2013, Mata Vaishnodevi University, Katra, India, DOI 10.1109/ICMIRA.2013.13, pp. 29 – 36.

[14] Chikhaoui Fatima, Djebbari Ali, 2013, "New chaotic binary sequences with good correlation property using logistic maps", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 5, pp. 59-64.

[15] Deb Sunder Swami, Kandarpa Kumar Sarma, 2014, "A Logistic Map Based PN Sequence Generator for Direct-Sequence Spread-Spectrum Modulation System", International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp.780-784.

[16] AhmadBeirami, Hamid Nejati, Sergio Callegari, "Fundamental Performance Limits of Chaotic-Map Random Number Generators" , Fifty-second Annual Allerton Conference Allerton House, UIUC, Illinois, USA October 1 - 3, 2014, IEEE**,** pp.1126-1131

[17] Bozhen Cai, Guangyi Wang, Fang Yuan, "Pseudo Random Sequence Generation From a New Chaotic System", Proceedings of ICCT20 I 5, 2015 IEEE, pp. 863-867.

[18] Wimol San-Um, Patinya Ketthong,Winai Chankasame, Jeerana Noymanee, "A Cost-Effective True Random Bit Generator Using a Pair of Robust Signum-Based Chaotic Maps", Science and Information Conference 2015, July 28-30, 2015, London, UK, pp. 1305-1310.

[19] Kazuyoshi TSUCIDYAt, Yasuyuki NOGAMI,"Periods of Sequences Generated by the Logistic Map over Finite Fields with Control Parameter Four", Proceedings of IWSDA' 15, 2015 IEEE, pp.155-159.

[20] Dimo Malchev, Ilhan Ibryam, 2015, "Construction of Pseudorandom Binary Sequences Using Chaotic Maps", Applied Mathematical Sciences, Vol. 9, No. 78, pp.3847 – 3853**.**

[21] Ajinkya H. Wanzkhade1 and Minakshee M. Patil, 2016, "FPGA implementation of direct sequence spread spectrum transmitter with pseudo chaotic generator", International Journal of Advanced Research, Volume 4, Issue 2, ISSN 2320-5407, pp.1020-1026.

[22] Lingfeng Liu1, Suoxia Miao, Hanping Hu, Yashuang Deng, 2016, "Pseudorandom bit generator based on non-stationary logistic maps", IET Inf. Information Security, Vol. 10, Iss. 2, pp. 87–94.

[23] Kaparapu Babulu and Battula Tirumala Krishna, "Generation of Phase Coded Pulses using Generalized Logistic maps", Third Asian Conference on Defence technology, 978-1-5090-4791-8/17 ©2017 IEEE.

[24] Bing Liu and Qiang Chen, "A Method of Generating Pseudorandom Binary Sequences Based on 3D Chaotic Mapping", 3rd International Conference on Information Management, 978-1-5090-6306-2/17 ©2017 IEEE.

[25] Alaa Kadhim. F and Hakeem Imad Mhaibes, 2018, "A Low-Cost True Random Bits Generator Based on Chaotic system and light nature", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5, pp. 2141-2146.

[26] M. Y. Mohamed Parvees, J. Abdul Samath and B. Parameswaran Bose, 2018, "The Role of Improved Logistic Map in Image Encryption", International Journal of Pure and Applied Mathematics, Volume 119, No. 16, pp. 491-500.

[27] Mahalinga V. Mandi, Ramesh S, Santosh Kulal, Santosh Kumar S, Dileep D, Yajnesh Padiyar, 2009, "An FPGA Implementation of a Pseudo-Chaotic Direct Sequence Spread Spectrum (DS-SS) Communication System", International Journal of Non-Linear Science (IJNS), Vol. 8, No. 4, pp. 387 – 401.

[28] Mahalinga V. Mandi, Ramesh S, Shivaputra, Dileep D, 2010, "Water Marked Image Encryption Using Logistic Map", International Journal of Computer Network and Security (IJCNS), Vol. 2, No.1, ISSN 0975-8283, pp 91 – 95.

[29] Mahalinga V. Mandi, Ramesh S, Shivaputra, Dileep D, 2010, "Implementation of Chaos Based Secured Communication System on 64x+ DSP", International Journal of Computer Network and Security (IJCNS), Vol. 2, No.1, ISSN 0975-8283, pp. 42 – 46.

[30] Mahalinga V. Mandi, K. N. Haribhat, R. Murali, 2010, "Generation of Large Set of Binary Sequences Derived from Chaotic Functions with Large Linear Complexity and Good Cross Correlation Properties", International Journal of Advanced Engineering and Applications (IJAEA), June 2010, Vol. III, pp. 313 – 322.

[31] Mahalinga. V. Mandi, K.N. Haribhat and R. Murali, 2006, "Generation of Discrete Spreading Sequences using Chaotic functions and their use in spread spectrum communication", Proceedings of the Sonata International Conference on Computer, Communication and Controls, 23rd-25th November 2005, pp. 128-133.

[32] Mahalinga. V. Mandi, K. N. Haribhat and R. Murali, 2006, "Chaotic functions for generating binary sequences and their suitability in Multiple access, Proceedings of the IEEE International Conference on Communication Technology, Vol. 1, pp. 217-220.