Munir, Fahad A.; **Zia, Muhammad**; **Mahmood, Hasan**

Designing multi-dimensional logistic map with fixed-point finite precision. (English)

Zbl 1430.68094
Nonlinear Dyn. 97, No. 4, 2147-2158 (2019).

Summary: In cryptographic algorithms, random sequences of longer period and higher nonlinearity are always desirable in order to increase resistance against cryptanalysis. The use of chaotic maps is an attractive choice as they exhibit properties that are suitable for cryptography. In continuous phase space of the logistic map, proper control parameters and initial state result into aperiodic trajectories. However, when the phase space of the logistic map is quantized, the trajectories terminate in finite and stable periodic orbits due to quantization error. The dynamic degradation of the logistic map can be mitigated using nonlinear feedback and cascading multiple chaotic maps. We propose a logistic map-based, finite precision multi-dimensional logistic map, that incorporates nonlinear feedback and modulus operations to perturb the chaotic trajectories. We present complexity, average cycle length and randomness analysis to evaluate the proposed method. The simulation results and analysis reveal that the proposed MDLM approach achieves longer period and higher randomness.

MSC:

68P25 Data encryption (aspects in computer science)
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
81P94 Quantum cryptography (quantum-theoretic aspects)

Keywords:

digital chaotic map; multi-dimensional logistic map; finite precision; chaotic maps; fixed-point processing

Software:

Diehard; Matlab

Full Text: DOI

References:

[1] Kolumban, G.: Theoretical noise performance of correlator-based chaotic communications schemes. IEEE Trans. Circuits Syst. I Fundam. Theory Appl. 47(12), 1692-1701 (2000) · Zbl 0984.94003

[2] Quyen, N.X., Yem, V.V., Hoang, T.M.: A chaos-based secure direct-sequence/spread-spectrum communication system. Abstr. Appl. Anal. 2013, 11 (2013) · Zbl 1322.94004

[3] Wang, S., Liu, W., Lu, H., Kuang, J., Hu, G.: Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications. Int. J. Mod. Phys. B 18(17n19), 2617-2622 (2004)

[4] Wang, S., Kuang, J., Li, J., Luo, Y., Lu, H., Hu, G.: Chaos-based secure communications in a large community. Phys. Rev. E 66(6), 065202 (2002)

[5] Heidari-Bateni, G., McGillem, C.D.: A chaotic direct-sequence spread-spectrum communication system. IEEE Trans. Commun. 42(234), 1524-1527 (1994)

[6] Lau, F.C., Chi, K.T.: Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods and Performance Evaluation. Springer, Berlin (2013)

[7] Zidan, M.A., Radawan, A.G., Salama, K.N.: Random number generation based on digital differential chaos. In: Proceedings of IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1-4 (2011)

[8] Matthews, R.: On the derivation of a chaotic encryption algorithm. Cryptologia 13(1), 29-42 (1989)

[9] Vlad, A., Luca, A., Hodea, O., Tataru, R.: Generating chaotic secure sequences using tent map and a running-key approach. Proc. Rom. Acad. Ser. A 14(Special Issue), 295-302 (2013)

[10] Kocarev, L.: Chaos-based cryptography: a brief overview. IEEE Circuits Syst. Mag. 1(3), 6-21 (2001)

[11] Li, C., Xie, T., Liu, Q., Cheng, G.: Cryptanalyzing image encryption using chaotic logistic map. Nonlinear Dyn. 78(2), 1545-1551 (2014)

[12] Strogatz, S.H.: Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering, 2nd edn.

Perseus Books Group, New York City (2014) · Zbl 1343.37001

[13] Khan, M., Shah, T., Mahmood, H., Gondal, M.A., Hussain, I.: A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dyn. 70(3), 2303-2311 (2012)

[14] Deng, Y., Hu, H., Xiong, W., Xiong, N.N., Liu, L.: Analysis and design of digital chaotic systems with desirable performance via feedback control. IEEE Trans. Syst. Man Cybern. Syst. 45(8), 1187-1200 (2015)

[15] Persohn, K.J., Povinelli, R.J.: Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. Chaos Solitons Fractals 45(3), 238-245 (2012)

[16] Guo, J.: Analysis of chaotic systems. http://math.uchicago.edu/May/Reu2014/Reupapers/Guo.Pdf (2014). Accessed 22 Aug 2017

[17] Beck, C.: Scaling behavior of random maps. Phys. Let. A 136(3), 121-125 (1989)

[18] Li, C., Lin, D., Lü, J., Hao, F.: Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. IEEE Multimed 25(4), 46-56 (2018)

[19] Li, C., Lin, D., Feng, B., Lü, J., Hao, F.: Cryptanalysis of a chaotic image encryption algorithm based on information entropy. IEEE Access 6, 75834-75842 (2018)

[20] Wheeler, D.D.: Problems with chaotic cryptosystems. Cryptologia 13(3), 243-250 (1989)

[21] Li, C.Y., Chen, J.S., Chang, T.Y.: A chaos-based pseudo random number generator using timing-based reseeding method. In: Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS), pp. 21-24 (2006)

[22] Wang, Q., Yu, S., Li, C., Lü, J., Fang, X., Guyeux, C., Bahi, J.M.: Theortical design and FPGA-based implementation of higher-dimensional digital chaotic systems. IEEE Trans. Circuits Syst. I Regul. Pap. 63(3), 401-412 (2016)

[23] Liu, L., Miao, S.: A universal method for improving the dynamical degradation of a digital chaotic system. Physica Scripta 90(8), 085205 (2015)

[24] Liu, Y., Luo, Y., Song, S., Cao, L., Liu, J., Harkin, J.: Counteracting dynamical degradation of digital chaotic chebyshev map via perturbation. Int. J. Bifurc. Chaos 27(3), 1750033 (2017) · Zbl 1360.37090

[25] Liu, L., Liu, B., Hu, H., Miao, S.: Reducing the dynamical degradation by bi-coupling digital chaotic maps. Int. J. Bifurc. Chaos 28(5), 1850059 (2018) · Zbl 1390.37058

[26] Garcia-Bosque, M., Pérez-Resa, A., Sánchez-Azqueta, C., Adlea, C., Celma, S.: Chaos-based bitwise dynamical pseudorandom number generator on FPGA. IEEE Trans. Instrum. Meas. 68(1), 291-293 (2018)

[27] Sprott, J.C.: Numerical Calculation of Largest Lyapunov Exponent. http://sprott.physics.wisc.edu/chaos/lyapexp.htm (2015). Accessed 11 Feb 2017

[28] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. Tech. rep., DTIC Document (2001)

[29] L'Ecuyer, P., Simard, R.: A C Library for Emperical Testing of Random Number Generators. ACM Trans. Math. Softw. (TOMS) 33(4), Art. no. 22 (2007)

[30] Marsaglia, G.: DIEHARD: a battery of tests of randomness. http://stat.fsu.edu/geo (1996)

[31] Li, C., Feng, B., Li, S., Kurths, J., Chen, G.: Dynamic analysis of digital chaotic maps via state-mapping networks. IEEE Trans. Circuits Syst. I Regul. Pap. 66(6), 2322-2335 (2019)

[32] Kantz, H., Schreiber, T.: Nonlinear Time Series Analysis, 2nd edn. Cambridge University Press, Cambridge (2004) · Zbl 1050.62093

[33] Siu, S.W.K.: Lyapunov Exponent Toolbox. https://www.mathworks.com/matlabcentral/fileexchange/233-let (1998). Accessed 15 Mar 2017

[34] Papoulis, A., Pillai, S.U.: Probability, Random Variables and Stochastic Processes, 4th edn. Tata McGraw-Hill Education, New York City (2002)

[35] Li, W., Songs, B., Ding, Q.: Discrete chaos circuit random characteristic analysis. In: Proceedings of IEEE 3rd International Conference on Robot, Vision and Signal Processing (RVSP), pp. 280-284 (2015)

[36] Chapra, S.C.: Applied Numerical Methods with Matlab: For Engineers and Scientists, 3rd edn. Tata McGraw-Hill Education, New York City (2007)

[37] Warner, S., Costenoble, S.R.: Finite Math and Applied Calculus, 6th edn. Cengage Learning, Boston (2013)