THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 21, Number 1/2020, pp. 29–36

NIST TESTS, LYAPUNOV EXPONENTS AND BIFURCATION DIAGRAMS WHEN EVALUATING CHAOS-BASED PRNGS

Octaviana DATCU, Adina-Elena LUPU (BLAJ), Tudor BLAJ, Radu HOBINCU

University "Politehnica" of Bucharest, Electronics, Faculty of Telecommunications and Information Technology
Corresponding author: Octaviana DATCU, E-mail: octaviana.datcu@upb.ro

Abstract. In order to determine if the behavior of a generator is random enough to be used in cryptographic applications, one can use the well-known NIST (National Institute of Standards and Technology) randomness test suite. In our previous work, we were empirically lead to the idea that the randomness or the lack of randomness affirmed by the well-known NIST tests can also be determined through the analysis of some chaos theory specific tools like the Lyapunov largest exponents and the bifurcation diagrams. In this paper we perform an experimental study to show how NIST tests and the Lyapunov exponents and bifurcation diagrams can cooperate when evaluating the randomness of chaos based pRNGs. We analyze five such pRNGs found in existing literature to establish a good foundation for our work. The conclusion is that the analysis by means of Lyapunov exponents and the bifurcation diagrams is a requirement in order to select the dynamic system parameters to design chaos-based pRNGs. However, only a good selection of the chaotic system parameters is not enough, the pRNG randomness quality depends on the generator design and must be evaluated by other methods, therefore the use of NIST Statistical Test Suite is highly important. Also, in the first part of the paper previous results are enriched with new details.

Key words: chaos-based pRNGs, Lyapunov exponents, bifurcation diagrams, NIST tests, private communications.

1. INTRODUCTION AND PROBLEM STATEMENT

A necessary condition for a good chaos-based pseudo random number generator (pRNG) is that the evolution of the underlying system is chaotic. The system must be non-periodic and highly sensitive to the initial state. Here, for the initial state of the pRNGs we use the standardized term, i.e. seed. The seed is composed of bifurcation parameters and initial values of the states of the system. This is the form that can guarantee the largest possible seed space.

Some of our results when evaluating chaos-based pRNGs were presented in [1,2]. The three-dimensional Hénon map [3,4] in (1), with a in $(0,2)$, b in $(-0.3, 0.3)$ and x, y, z in $(-2, 2)$, was used to generate three floating-point time series. The pRNG took the last significant byte of the samples from the three-time series, x_k, y_k, z_k and added them modulo two without carry, resulting in a new byte.

$$x_{k+1} = a - y_k^2 - bz_k\,; \quad y_{k+1} = x_k\,; \quad z_{k+1} = y_k\,. \tag{1}$$

Given the definition intervals for (1) and working in double precision floating point [5], the seed space could have 6.6×10^{15} elements. While evaluating the resulted pRNG, the authors observed a close correspondence between the randomness affirmed by the well-known NIST [6] tests and the analysis of some chaos theory specific tools, the Lyapunov largest exponents [7] and the bifurcation diagrams [8]. From this observation, the question arose whether these chaos specific metrics could be helpful in determining the degree of randomness of chaos based pRNGs knowing the initial conditions and parameters. Most generator proposals promote valid initial states, from which the system exhibits chaotic behavior. For the generalized Hénon map, the literature specifies a valid pair of parameters (a, b) to be $(1.76, 0.1)$. We could settle on that pair and fix the values, greatly decreasing the seed space of the generator - an important parameter for cryptographic pRNGs. One of the approaches to mitigate this issue is dynamically changing the parameters during runtime. Thus, even if the initial state is not valid, the generator will not be stuck in a pattern or on a

fixed value. Another method would be to filter the selected parameters depending on some easy-computable metrics. This is where the present research might be of use.

2. EVALUATION OF SOME CHAOS-BASED PRNGS

2.1. More details on the generalized Hénon map based pRNG

In this paper, the parameter b of the three-dimensional Hénon map is fixed at 0.1, initial conditions at $x_0 = y_0 = z_0 = 0$ and a is varied in its entire definition domain, $(0, 2)$, with a step of 10^{-3}. The bifurcation diagram and Lyapunov exponents are depicted in Fig. 1. From the two images, one would say that the valid seed space for parameter a is $K_a = [0.786, 1.077] \cup [1.4, 1.76]$. For the subinterval $[0.786, 1.077]$ the largest Lyapunov exponent is almost zero, implying stability of the Hénon map (1). For the computation step 10^{-3}, for three of the values in $[1.4, 1.76]$ the largest Lyapunov exponent is negative, meaning these values do not form a valid pair with the parameter $b = 0.1$. As the computation step is decreased, in Fig. 2, 10^{-4} reveals nine values of the parameter a that, when $b = 0.1$, take system (1) in a periodic regime ($\lambda_1 < 0$). When going deeper, at 10^{-5}, the number of pairs that do not engender chaos is more than one hundred.

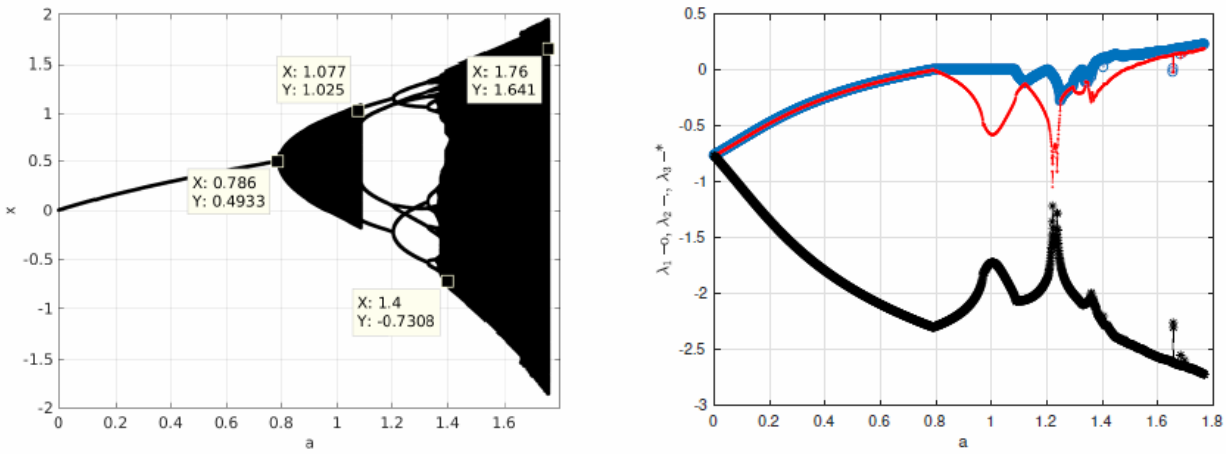

Fig. 1 – Bifurcation diagrams (left) and Lyapunov exponents (right) for the Hénon map using a computation step of 10^{-3}. λ_1 in blue, λ_2 in red, λ_3 in black.

Table 1 gives the approximate magnitude order and the signum for the Lyapunov exponents for a in $[0.8, 0.9]$. A NIST test suite is also run for $b = 0.1$, $x_0 = y_0 = z_0 = 0$ and a in K_a, with a step of 10^{-3}; results are summarized in Table 2. The number in parenthesis points to the number of the failed tests from that category. We were intrigued by the fact that some of the pairs resulted in zero NIST tests failed, even if the Lyapunov exponents are very close to zero, but still positive. For example, $a = 0.803$ gives $\lambda_1 = 10^{-6}$. All NIST tests were passed, but the pair $(a, b) = (0.803, 0.1)$ results in the attractor in Fig. 3 (left).

When compared to the attractor engendered by $(a, b) = (1.75, 0.1)$, one can see the tendency of the iterations to form a closed periodic orbit. This relation between close to zero values of the greatest Lyapunov exponent and the pRNG passing all NIST tests must be analyzed in a future work.

Table 1

The Lyapunov exponents of the Hénon map for b = 0.1 and varying a in [0.8, 0.9]

a	λ_1	λ_2	λ_3
0.800 - 0.802, 0.806, 0.807, 0.809, 0.810, 0.813, 0.816 - 0.820, 0.824 - 0.826, 0.828, 0.831, 0.833 - 0.835, 0.841, 0.842, 0.844, 0.845, 0.846, 0.848, 0.850, 0.854, 0.858 - 0.863, 0.867, 0.869, 0.871, 0.875, 0.877, 0.879, 0.880, 0.883-0.885, 0.889, 0.891, 0.897 - 0.900	10^{-5}	10^{-2}	–2
0.803 - 0.805, 0.808, 0.811, 0.812, 0.814, 0.815, 0.821 - 0.823, 0.827, 0.829, 0.830, 0.832, 0.836 - 0.840, 0.843, 0.847, 0.849, 0.851 - 0.853, 0.855 - 0.857, 0.864, 0.865, 0.866, 0.868, 0,870, 0.872 - 0.874, 0.876, 0.878, 0.881, 0.882, 0.886 - 0.888, 0.889, 0.892 - 0.896	10^{-6}	10^{-2}	–2

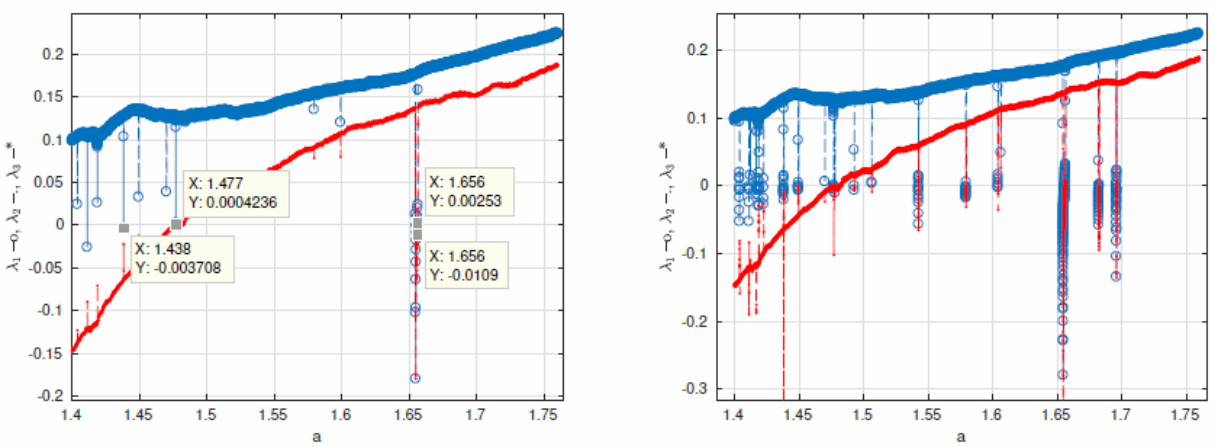

Fig. 2 – Zoom on the two largest Lyapunov exponents for the Hénon map. Computation step of 10^{-4} (left) and 10^{-5} (right). λ_1 in blue, λ_2 in red, λ_3 in black.

Table 2

The failed NIST tests for $b = 0.1$ and varying a

Failed NIST test	***a* in [0.8, 1.09]**	***a* in [1.4, 1.76)**
Frequency	0.888, 1.044, 1.088, 1.089, 1.090	1.404
Block Frequency	0.958, 0.996, 0.999, 1.026, 1.042, 1.071, 1.088, 1.089, 1.090	1.404, 1.427, 1.627, 1.655, 1.682
CumulativeSums (2 tests)	0.888, 0.988, 0.999, 1.007, 1.019 ***(1)***; 1.044, 1.088, 1.089, 1.090 ***(2)***	1.404 ***(2)***; 1.600, 1.655, 1.682 ***(1)***
Runs, LongestRun, Rank,	1.088, 1.089, 1.090	1.404, 1.655, 1.682
OverlappingTemplate		1.481, 1.655, 168, 1.726
Universal		1.404, 1.655, 1.682
FFT		1.404, 1.425, 1.505, 1.655, 1.682
NonOverlappingTemplate (148 tests)	0.819, 0.827, 0.828, 0.829, 0.834, 0.837, 0.853, 0.862, 0.864, 0.867, 0.868, 0.871, 0.880, 0.902, 0.904, 0.917, 0.918, 0.926, 0.928, 0.935, 0.937, 0.942, 0.943, 0.944, 0.947, 0.957, 0.979, 0.980, 0.984, 0.991, 1.000, 1.010, 1.021, 1.027, 1.032, 1.036, 1.054 ***(1)***; 0.815, 0.933, 1.037 ***(2)***; 0.812 ***(3)***; 0.840 ***(4)***; 1.088, 1.089, 1.090 ***(148)***	1.408, 1.411, 1.413, 1.418, 1.421, 1.423, 1.435, 1.447, 1.448, 1.451, 1.458, 1.461, 1.462, 1.486, 1.487, 1.493, 1.498, 1.502, 1.506, 1.511, 1.512, 1.514, 1.520, 1.529, 1.539, 1.544, 1.558, 1.584, 1.585, 1.594, 1.596, 1.597, 1.607, 1.623, 1.628, 1.630, 1.638, 1.641, 1.650, 1.470, 1.465, 1.658, 1.668, 1.672, 1.673, 1.679, 1.687, 1.691, 1.702, 1.727, 1.728, 1.733, 1.748, 1.753, 1.759, 1.481, 1.726 ***(1)***; 1.428, 1.523, 1.560, 1.632, 1.655, 1.682, 1.708, 1.723, 1.731, 1.537 ***(3)***; 1.404 ***(118)***
ApproximateEntropy	0.965, 0.975, 0.988, 0.996, 1.007, 1.022, 1.028, 1.030, 1.088, 1.089, 1.090	1.404, 1.578, 1.655, 1.682
Serial (2 tests)	0.995, 1.088 ***(1)***; 1.089, 1.090 ***(2)***	1.483, 1.701 ***(1)***; 1.404, 1.655, 1.682 ***(2)***
LinearComplexity	1.088, 1.089, 1.090	1.404, 1.655, 1.682
Random Excursions	0.865, 0.904, 1.043	

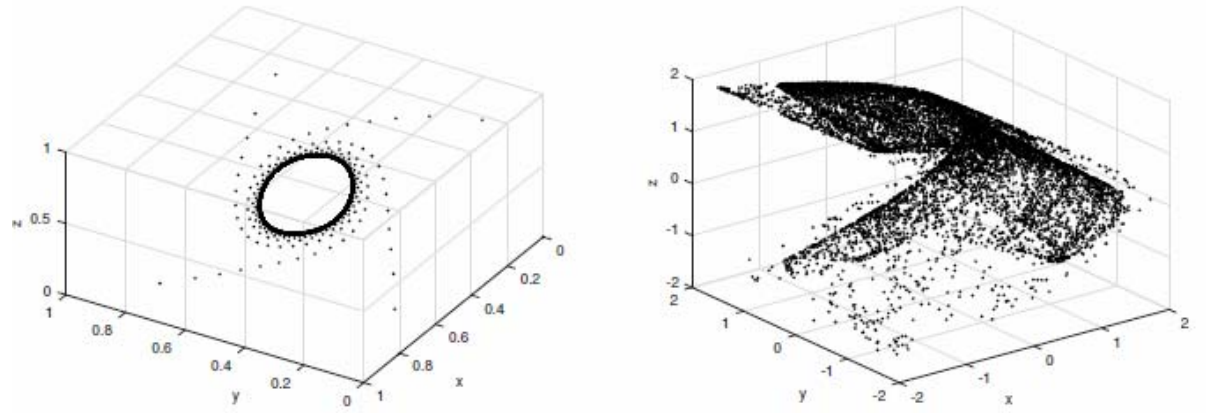

Fig. 3 – Attractors for the Hénon map for $b = 0.1$ and $a = 0.803$ (left) or $a = 1.75$ (right).

2.2. Analysis of some Chaos-Based pRNGs from the literature

To confirm or to disagree with that intuition affirmed by [1] the authors took some chaos-based pRNGs existing in the literature and confronted them to the same analysis as the above pRNG based on the three-dimensional Hénon map was. They are called Generator k, with $k=\{1,2\ldots,5\}$, for the ease of naming them in the remaining of the paper.

The algorithms used by the five pRNGs and the underlying (chaotic) systems are briefly described. These algorithms are implemented in Matlab 2017a and in C++[1]. Bifurcation diagrams and Lyapunov exponents were computed for each generator. Values for the parameters of the underlying maps/flow engendering chaotic or periodic behavior were chosen and NIST tests were run as they were for the Hénon map based pRNG. Conclusions regarding the utility of this approach to accelerate the evaluation of chaos-based pRNGs are drawn in the final section.

GENERATOR 1 [9] proposes a new technique to improve the randomness properties of chaos-based cryptosystems. This technique has been applied to an algorithm based on a skew tent map (2). The improvement consists in using a set of different values for the chaotic parameter.

$$x[k+1]=\begin{cases}\dfrac{x[k]}{\gamma}, & x[k]\in(0,\gamma),\\ \dfrac{1-x[k]}{1-\gamma}, & x[k]\in(\gamma,1).\end{cases} \tag{2}$$

GENERATOR 2 [10] combines the piecewise linear chaotic map (3) with the logistic map (4), with $x[k]$ in (0,1) and b in (0,4]. A set of transformations is applied to the two chaotic maps, then a bitwise XOR operation is applied between the transformed chaotic maps.

$$x[k+1]=\begin{cases}\left(\dfrac{5}{2}\right)x[k], & x[k]\in[0,2),\\ x[k]+3, & x[k]\in[2,5),\\ -\left(\dfrac{79}{30}\right)x[k]+\left(\dfrac{127}{6}\right), & x[k]\in[5,8),\\ -\left(\dfrac{1}{20}\right)x[k]+\dfrac{1}{2}, & x[k]\in[8,10].\end{cases} \tag{3}$$

GENERATOR 3 [11] is a pRNG based on the iteration of two logistic maps (4). The output of the pRNG is generated by comparing at each iteration the values of the two logistic maps. Based on the comparison between the values of the two, at each iteration, the output is either 1 or 0.

$$x[k+1]=bx[k]\left(1-x[k]\right),\ x[k]\in(0,1). \tag{4}$$

GENERATOR 4 [12] constructs a pRNG using two logistic maps and S-box (substitution boxes) tables. The output of this pRNG are 8-bit numbers.

GENERATOR 5 [13] presents a pRNG based on a new chaotic flow digitized with a DSP:

$$\mathrm{d}x/\mathrm{d}t=-ay+d^{z^2};\quad \mathrm{d}y/\mathrm{d}t=cy+x;\quad \mathrm{d}z/\mathrm{d}t=x-bz. \tag{5}$$

We have implemented all five generators both in Matlab 2017a – to plot bifurcation diagrams and Lyapunov exponents – as well as C++, to integrate the code with the statistical tests. The bifurcation diagrams and Lyapunov exponents for the maps used by GENERATORS 1-4, namely the skew tent map and the logistic map, are already known [4,14], so we do not show them in the present paper. As for GENERATOR 5, the test parameters in Table 3 are chosen from the indications given by the authors in [12], because the frequency used for sampling is not specified. We have selected several seed values (initial states

[1] https://gitlab.dcae.pub.ro/research/chaos/rcd-2019/tree/master

and parameters) that display chaotic behavior and some that do not. For these seed values we have run the NIST test battery. We expected to find a correspondence between results: only the seeds for which the bifurcation diagrams show many solutions and the largest Lyapunov exponent is positive, are the seeds that determine a low number of failed NIST tests.

Table 3

Results of NIST test suite with different values of parameters for GENERATORs 1-5

	Parameters	**Behavior**	**Failed runs**	**Corresponding**
GEN 1	γ = *rand*(0,1)	chaotic	1	Fig. 4 (top left)
GEN 2	b = 3.776	chaotic	1	Fig. 4 (top center)
	b = 2.7	periodic	161	Fig. 4 (bottom center)
GEN 3	b = 3.776	chaotic	154	Fig. 4 (top right)
	b = 3	periodic	158	Fig. 4 (bottom right)
GEN 4	b = 3.776	chaotic	12	Fig. 5 (first 2 images)
	b = 2.3	periodic	162	Fig. 5 (5^{th} and 6^{th} images)
GEN 5	a = 10, b = 3.5, c = 0.65, d = 4.7	chaotic	1	Fig. 5 (3^{rd} and 4^{th} images)
	a = 30, b = 2.5, c = 0.25, d = 6500	periodic	162	Fig. 5 (7^{th} and 8^{th} images)

The images in Fig. 4 and Fig. 5 illustrate results when enciphering the image using GENERATORs 1-5. With values for the control parameter(s) which engender chaotic behavior, we obtain proper encrypted images. This result along with the bifurcation diagrams and the largest Lyapunov exponent sustain the pseudo-randomness of the pRNGs. Otherwise, when using values for the control parameters that generate a non-chaotic behavior (as pointed out by the bifurcation diagrams and Lyapunov exponents) the results show inappropriate encrypted images and non-uniform histograms. This indicates the lack of pseudo-randomness of the generators.

3. CONCLUSION

In this paper, we have extended our analysis regarding the correspondence between the NIST statistical tests for pseudo-random number generators and specific chaotic metrics – Lyapunov exponents and bifurcation diagrams – as a possible way to validate chaos based pRNGs (and) seeds. More details were provided for our previous proposal of a generalized Hénon map based pRNG. As the computation step is decreased, when investigating the bifurcation parameters, more values for which the greatest Lyapunov exponent is negative (periodic behavior of the system) are revealed. These values must be removed from the seed space. Without a detailed study of the bifurcation diagrams and Lyapunov exponents, an unadvised user of a chaos based pRNG would be prone to choose an inappropriate seed. NIST tests would correct this wrong choice, but they are less accessible to the common user. Even if the NIST test suite is open source and their interpretation is available [14], the test battery is much more difficult to understand and to track than the chaos specific metrics previously mentioned.

We have also selected five proposed pRNG architectures and we have compared the NIST battery test results to the previously mentioned metrics. For the chaos-based generators which periodically change their bifurcation parameters (e.g. GEN 1, GEN 4) another approach must be devised since we cannot study the chaos specific metrics for a given value of the initial seed.

The results show a tight link between NIST tests and the chaos metrics. There are still inconsistencies that could be explained by the fact that the randomness of the sequences does not depend only on the chaotic state of the underlying system, but also on the post-processing and the pRNG architecture. Even though chaos-specific metrics are easy to implement and provide some initial hints on the quality of the selected parameters, they do not replace the statistical analysis of the resulted generator. Nevertheless, the present results show a promising approach to be investigated further.

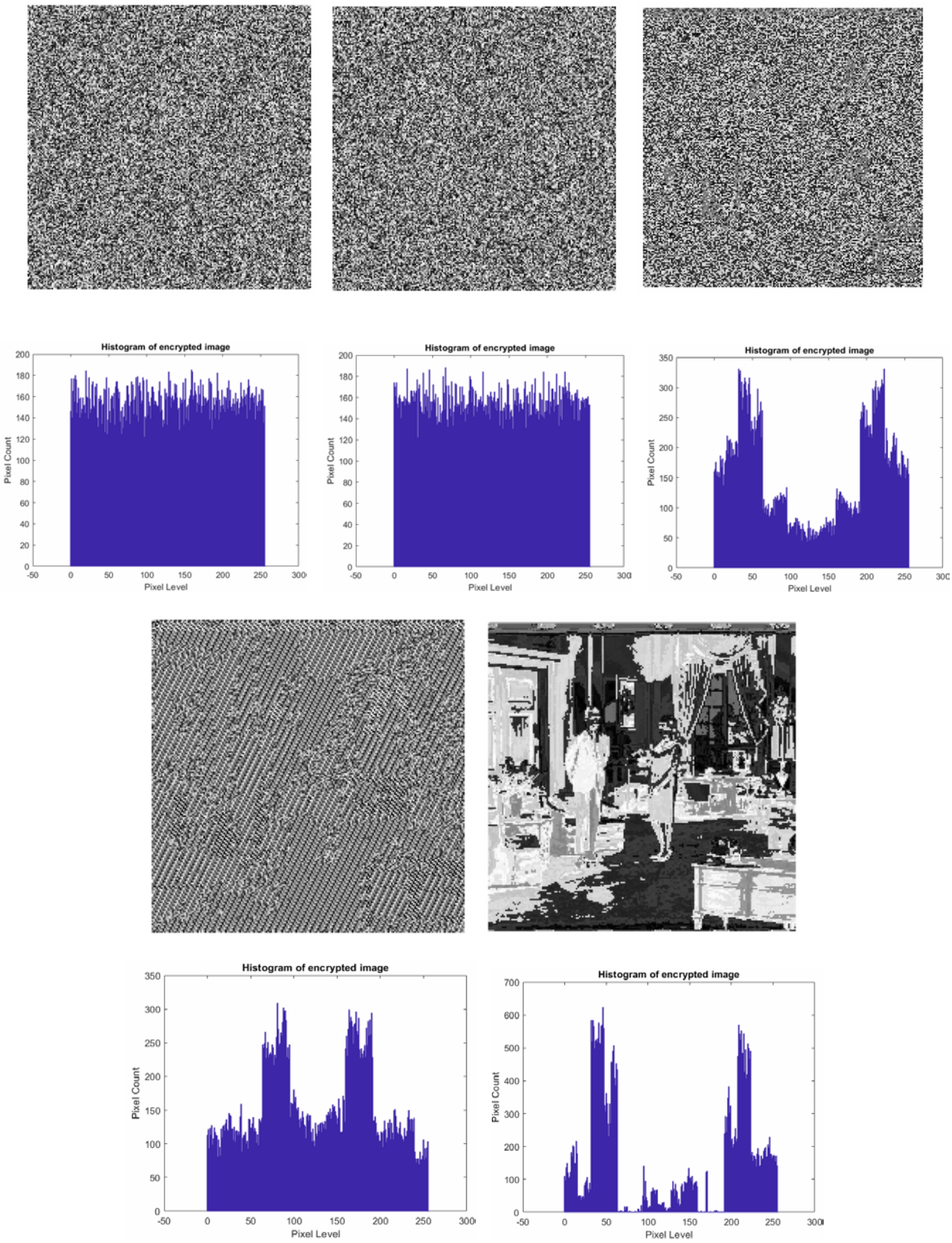

Fig. 4 – Results of encryption with each of the GENERATORS 1-3 for a suitable seed (top) and a bad one (bottom) and corresponding histograms for pixel values.

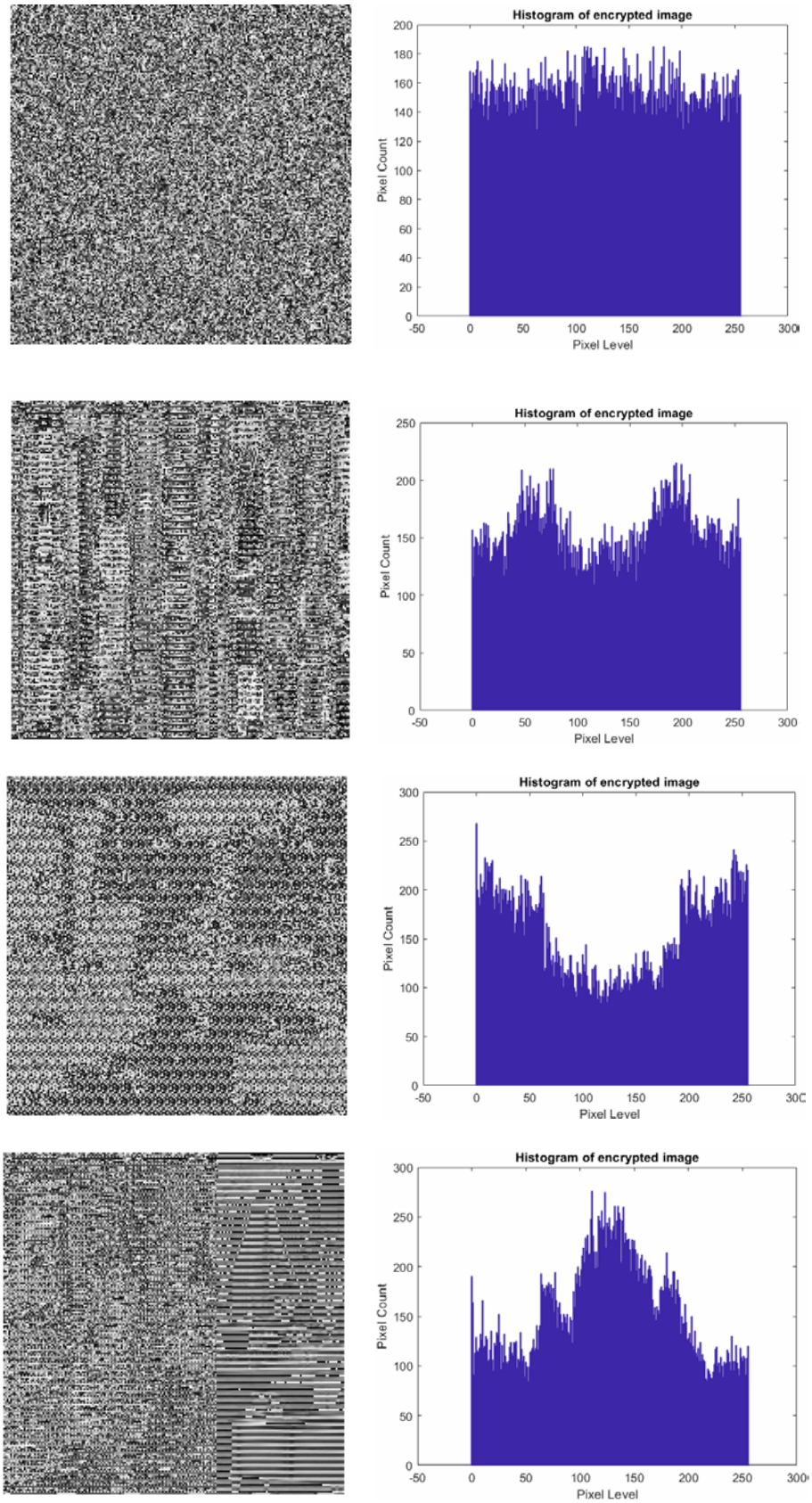

Fig. 5 – Results of encryption with each of the GENERATORS 4-5 and corresponding histograms for pixel values. Suitable seeds (first two rows) and non-suitable (last two rows).

REFERENCES

1. O. DATCU, R. HOBINCU, *NIST tests versus bifurcation diagrams and Lyapunov exponents when evaluating chaos-based pRNGs*, Proceedings of ITISE 2018, Granada, Spain, pp. 1640-1649.
2. R. HOBINCU, O. DATCU, *A novel chaos based pRNG targeting secret communication*, COMM 2018, Bucharest, Romania, June 2018.
3. D.A. MLLER, G. GRASSI, *A discrete generalized hyper chaotic Hénon map circuit*, Proceedings of the 44th IEEE 2001 Midwest Symposium on Circuits and Systems, Vol. **1**, pp. 328-331, 2001.
4. G. GRASSI, D.A. MILLER, *Theory and experimental realization of observer based discrete-time hyperchaos synchronization*, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, **49**, *3*, pp. 373-378, 2002.
5. *Standard for Floating-Point Arithmetic P754, version 1.2.5. Revising ANSI/IEEE Std 754-1985* (Report), October 4, 2006.
6. A. RUKHIN, J. SOTO, J. NECHVATAL, M. SMID, E. BARKER, S. LEIGH, M. VANGEL, D. BANKS, A. HECKERT, J. DRAY, SAN VO, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22, Revision 1a, 2010.
7. A. WOLF, J.B. SWIFT, H.L. SWINNEY, J.A. VASTANO, *Determining Lyapunov exponents from a time series*, Physica D, **16**, *3*, pp. 285-317, 1985.
8. S. STROGATZ, *Non-linear dynamics and chaos: with applications to Physics, Biology, Chemistry and Engineering*, Addison-Wesley, 1994.
9. M. GARCIA-BOSQUE, A. PÉREZ-RESA, C. SÁNCHEZ-AZQUETA, S. CELMA, *A new randomness-enhancement method for chaos-based cryptosystem*, 2018 IEEE 9th Latin American Symposium on Circuits & Systems, Puerto Vallarta, doi: 10.1109/LASCAS.2018.8399959.
10. L. MIN, K. HU, L. ZHANG, Y. ZHANG, *Study on pseudorandomness of some pseudorandom number generators with application*, 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, China, 2013, pp. 569-574, doi: 10.1109/CIS.2013.126.
11. V. PATIDAR, K.K. SUD, N.K. PAREEK, *A pseudo random bit generator based on chaotic logistic map and its statistical testing*, Informatica, **33**, *4*, pp. 441-452, 2009.
12. M.N.M. HAMDI, R. RHOUMA, S. BELGHITH, *A very efficient pseudo-random number generator based on chaotic maps and S-box tables*, World Academy of Science, Engineering and Technology, International Journal of Electronics and Comm. Engineering, **9**, *2*, pp. 481-485, 2015.
13. B. CAI, G. WANG, F. YUAN, *Pseudo random sequence generation from a new chaotic system*, 2015 IEEE 16th Int. Conf. on Comm. Technology (ICCT), Hangzhou, China, 2015, pp. 863-867.
14. M. SAIDI, H. HERMASSI, R. RHOUMA, S. BELGHITH, *LSB-hamming based chaotic steganography (LH-Steg)*, The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017), Cambridge, UK, December 2017, pp. 29-34.

Received July 10, 2019