# Improving Chaotic Generator's Speed Performance for Secure Information Transmitting

Oleg Garasym
*IRCCyN UMR CNRS 6597,*
*Ecole Centrale de Nantes*
*Nantes, France*

Ina Taralova
*IRCCyN UMR CNRS 6597,*
*Ecole Centrale de Nantes*
*Nantes, France*

## Abstract

*In this paper an improved Lozi system speed performance is achieved in application to chaotic switched model. Generally speaking, the main advantage of the switched encryption model is its robustness to the noise, while the main drawback is the slow processing speed. In this article we propose to gain model productivity by adjusting parameter in Lozi chaotic generator. Chaos generator is sensitive to any structure, therefore the solution shouldn't influence the pseudo randomness which is required for encryption. We provide the results of switched chaotic model based on Lozi chaotic generator with changeable parameter studied for chaoticity and pseudo-randomness with NIST, largest Lyapunov exponent, auto-correlation, cross-correlation and cumulative distribution.*

## 1. Introduction

The current cryptographic methods of processing information aim at increasing keys length that in turn reduce the cryptographic transformations performance in terms of processing time. This is especially critical to ensure a given level resistance to the implementation in special systems and devices with existing restrictions on the amount of memory and dimensions in cases where there is no possibility to use powerful processing devices. This fact determines the importance and relevance of the search for methods to improve cryptosystem security level, robustness and speed performance.

Pseudo random number generators (PRNG) play very important cryptographic role. They are used for information encryption, to generate the encryption keys and the initialization vectors authentification requests, for the formation of a common key generating prime numbers. If PRNG is hacked, in most cases, the entire security of the system can be under threat.

Chaotic systems that generate pseudo random sequences are attracting attention, due to their complex, aperiodic and chaotic behavior and because they are sensitive to small changes in initial values and control parameters. However, using a digital system to generate chaos has many difficulties. For example, chaos is restrained by the finite precision of the system and even small errors introduced in each iteration will have a big effect on the implementation of chaos [1, 2]. Consequently, the accumulation of the error will result in a deviation of the orbit and greatly affects the characteristics of the system. Due to the reactiveness of the chaos to initial conditions and parameters, chaotic key stream is easily affected by environmental conditions [3].

Chaotic sequences are produced by nonlinear dynamic systems that increase PRNG complexity. Nowadays many random number generators in use do not always produce sequences that are sufficiently random and usually generate very repetitive patterns, if lots of runs are required. Randomness' tests in data evaluation are used to analyze the distribution pattern of a data set. In stochastic modeling, as in some computer simulations, the expected random input data can be verified to show that tests were performed using randomized data [4]. Chaos-based PRNG is interesting application for the control theory development but always take around on open problem how to satisfy each of the requirements: robustness, security and speed performance.

In this paper we consider 3 basic models with chaotic implementation to secure information transmitting. The models performance and their advantages, disadvantages are described in the section 2. In the section 3 the problem statement is explained and in section 4 the proposed solution is proposed. Section 5 explains new parameter influence on chaotic generator's randomness and robustness. In section 6 systems results (original and after modification) are compared. Future work, results and summery end the paper.

## 2. Chaos-based encryption models

There are three basic encryption schemes: CS (Chaotic Switching), CMI (Chaotic Mixing) and CMA (Chaotic Masking) (fig.1) [5]. In CS the message is encoded by switching the transmitter between two states. CMI is based on the modulation of chaotic carrier generated by the transmitter.

Finally in CMA the encoding is achieved by adding the message to the chaotic transmitter output.

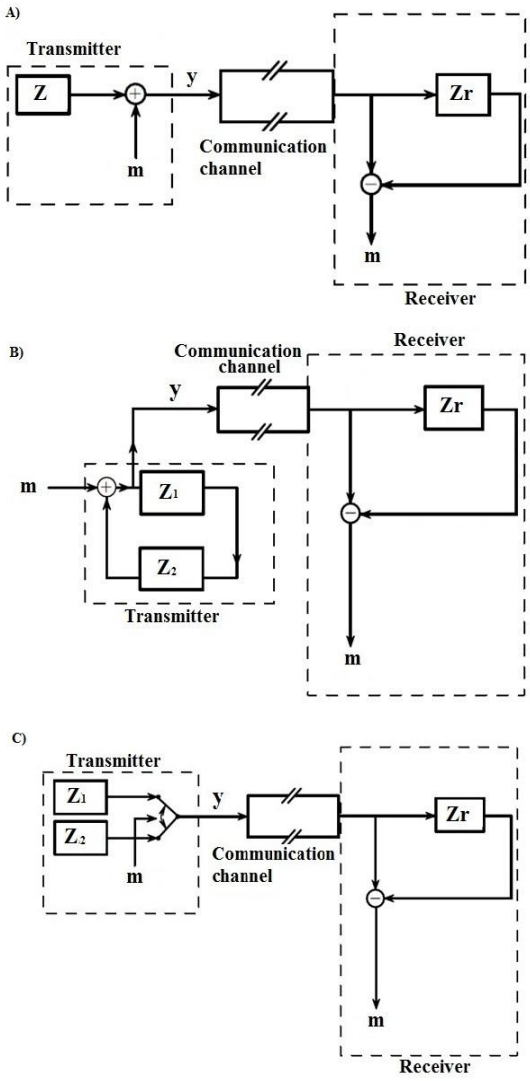


**Figure1. A) Chaotic masking; B) Nonlinear mixing of information signal to chaotic; C) Switched chaotic model**

## 2.1. Chaotic masking (CMA)

On the transmitting side (fig.1-A) information signal $m$ is mixed to the carrier signal generated by the emitting chaotic system $z$, and then transmitted over the communication channel.

The receiver $z_r$ is performing a full chaotic synchronization of the chaotic generator and the receiver, resulting in a dynamic host generator behavior that becomes identical to the transmission dynamics.

**2.1.1. Advantages.** This hidden communication model works quite efficiently. It allows the transmission of information to be qualitatively performed and the detection of its output in the absence of noise in the channel when the power of the signal generated by the transmitter system exceeds the power of the information signal.

**2.1.2. Disadvantages.** Adding noise to the communication channel leads to a sharp deterioration in the quality of transmitted information, requiring a high signal / noise ratio at which the scheme is working. Furthermore, the control parameters mismatch between identical chaotic generators (but located on different sides of the communication channel) also leads to additional noise at the output of desynchronization and makes information transfer difficult to fulfill. Moreover, there is the issue of confidentiality of information transfer.

## 2.2. Chaotic mixing (CMI)

The transmitting side contains two identical chaotic generators, $z_1$ and $z_2$ (fig. 1-B). The information signal $m$ is mixed with the signals produced by $z_1$ and output is mixed with $z_2$. As a result of passing the feedback (provided by mutual generators coupling) the signal undergoes nonlinear changes. Thus, the communication channel is the transmitted signal $y$ obtained by nonlinear mixing of information signal to the chaotic. The receiving device, as in the above scheme, contains a chaotic generator $z_r$, identical to the ones in the transmitter. The receiver synchronizes the generator in case of transmission of binary bits 0 (and does not synchronize the transmission of binary bits 1).

**2.2.1. Advantages.** An important advantage of such schemes to the scheme based on chaotic masking is the ability to vary the level of the input data message, allowing to control the quality of information transfer.

**2.2.2. Disadvantages.** Increasing the quality of communication entails a loss of confidentiality that is a significant drawback. In addition, this model is characterized by a low resistance to noise in the communication channel and mismatch control parameters of the initially identical chaotic generators. The need to ensure the identity of the three chaotic generators, two of which are located on opposite sides of the communication channel is an intractable technical problem and, therefore, is another drawback of this scheme.

## 2.3. Switched chaotic model (CS)

The transmitting device consists of two chaotic generators $z_1$ and $z_2$ (fig.1-C) that may be identical

(only started from different initial condition), however, in the interest of confidentiality of data transmission it is preferable to use different generators' parameters. Moreover, the signals generated by these systems must have similar spectral and statistical properties. A digital message $m$, represented by a sequence of binary bits 0/1 is encoded by chaotic generators output switching. For example the output signal from the first random generator is chosen when $m$ is equal to 0; when $m$ is equal 1 the second random generator is selected. Thus the obtained switched signal $y$ is transmitted over the communication channel to the receiver $Z_r$. Depending on the number of generators that are on the receiving side of the channel, there are several schemes of secure communication based on chaotic switching modes.

**2.3.1. Advantages.** The switched encryption model is more resistant to the noise in the communication channel than the chaotic masking scheme or the nonlinear signal mixing model. And it has been proven in [6] that chaotic generators combination makes chaotic behavior more complex.

**2.3.2. Disadvantages.** The principal drawback of this model is the occurrence of switching transients (the length of which can be quite time-consuming), that impacts the delay time in the synchronous mode of the receiving generator. Therefore, these schemes can be quite slow and also they have weak security [7].

## 3. Problem statement

Hereafter we propose an improved version of Lozi chaotic generator to switched encryption model (CS) that ensures better speed performances and robustness. The two chaotic generators $Z_1$ and $Z_2$ used for encryption are analyzed to setter: long-cycle length; high complexity; auto-correlation, cross-correlation near to zero; balance on [-1 1]; largest Lypunov exponent; successful NIST test [8]. In theory there is an endless number of sequences, for $Z_1$ or $Z_2$ chaotic system, each realizable by changing the initial conditions. A slight difference in the initial conditions between transmitter and receiver will produce very different modulation and demodulation codes, which is an advantage of a secure chaos-based communication system.

The problem is that noise in the communication channel leads to errors in the receiver's part. Thus there is no perfect model of using chaotic generator for secure message transmission.

The proposed model to use for secure information transmission is CS that has better resistance to the noise in the communication channel than other models. The security problem that is considered in [7] can be solved in combination with other models.

To construct the model we consider a new Lozi alternate system with auto-coupling and ring-coupling proposed in (2011) [9] and described in [10] that has very satisfactory chaotic properties on the p-dimensional torus, $x\in R^p \quad T^p=[-1,\ 1]^p$ by the map $M_p: T^p \Rightarrow T^p$.

$$z:\begin{cases} x_{n+1}^1 = 1-2\left|x_n^1\right| + k^1((1-e_1)x_n^2 + e_1 x_n^1) \\ x_{n+1}^2 = 1-2\left|x_n^2\right| + k^2((1-e_1)x_n^3 + e_2 x_n^2) \\ \vdots \\ x_{n+1}^p = 1-2\left|x_n^p\right| + k^p((1-e_p)x_n^p + e_p x_n^p) \end{cases} \quad (1)$$

Where the parameters $k^j=(-1)^{j+1}$, and smaller epsilon guarantee weak coupling $e_p \in ]0,1[$. The graph of the map $-2\left|x_n^p\right|$ is the tent map. To avoid divergence, the escaping trajectories have to mapped back to the torus $T^p=[-1,1]^p$ :

$$\text{If } x_{n+1}^j = 1-2\left|x_n^j\right| + k^j((1-e_j)x_n^{j+1} + e_p x_n^j) < -1$$

then add 2

$$\text{If } x_{n+1}^j = 1-2\left|x_n^j\right| + k^j((1-e_j)x_n^{j+1} + e_p x_n^j) > 1 \text{ then}$$

substract 2

However another problem with chaotic systems is autonomy and any modification in the system could lead to loss of randomness. Hence the aim is to simplify the applied model while maintaining security and increasing work-speed.

## 4. Solving the problem

We suggest that instead of switching between two different independent generators, to change only the parameters of the same generator (structurally speaking) depending on the message bit (0 or 1). The chaotic system sensitivity allows us to slightly change parameters in order to create generators with new dynamical properties. The question is if the new generator will have the same good characteristics of randomness and chaoticity.

We investigated the system (1) and propose to add a switching parameter *a*.

$$a=\begin{cases} 1 & ,m_n=1 \\ d & ,m_n=0, \quad where \quad d<1 \end{cases}$$

where $m_n$ is a bit of a message and equal to 1 or 0. The new parameter *a* is added to the system (1):

$$\begin{aligned} x^1_{n+1} &= 1 - 2\left|x^1_n\right| + ak^1((1-e_1)x^2_n + e_1 x^1_n) \\ x^2_{n+1} &= 1-2\left|x^2_n\right| + ak^2((1-e_2)x^3_n + e_2 x^2_n) \\ &\vdots \\ x^p_{n+1} &= 1 - 2\left|x^p_n\right| + ak^p \frac{((1-e_p)x^1_n + e_p x^p_n)}{\mu} \end{aligned} \quad (2)$$

$$\text{If } x^j_{n+1} = 1 - 2\left|x^j_n\right| + ak^j((1-e_j)x^{j+1}_n + e_p x^j_n) < -1$$

$$\text{then add 2} \quad (3)$$

$$\text{If } x^j_{n+1} = 1 - 2\left|x^j_n\right| + ak^j((1-e_j)x^{j+1}_n + e_p x^j_n) > 1$$

$$\text{then substract 2}$$

where *a* is a parameter of the chaotic system that changes depending on the bit of the message $m_n$. For encrypting bit '1' of the binary message a=1 (Lozi system) and for bit '0' a= d, where d<1 (modified Lozi system). Moreover the additional parameter allows to increase the size of the encryption key.

To confirm system complexity we use largest Lyapunov exponent. The latter is used to prove chaos existence in the system [11]. A positive largest Lyapunov exponent indicates chaos and the value of this index defines the degree of chaoticity. Lyapunov exponent characterizes the average rate of exponential divergence of close phase trajectories. If $d_0$ is an initial distance between two initial points of the phase trajectories in time *t* distance between trajectories, that go out of this points will be: $d(t)=d_0 e^{\lambda t}$, where $\lambda$ is called the Lyapunov exponent. Each dynamical system is characterized by spectrum Lyapunov exponent $\lambda_i (i = 1,2,\ldots,n)$ where n is an equation number needed for system description and if $\lambda$ is bigger the chaoticity is stronger.

The aforementioned methods for analyzing randomness give the possibility to determine chaotic generators quality and security.

To check the system for chaos exsistence Largest Lyapunov Exponent (LLE) approach is applied by using free software package TISEAN [12]. The sequence must be saved in ASCII format and after that is called the function by lyap _r from matlab:

*system([tiseanPath, 'lyap_r -s20 -o lyapunov.dat Lozi_m.dat']);*

The LLE for Lozi system is equal 0.6599, for modified Lozi system where a=0.1 is 0.7232.

For p-dimensional systems, where p>=2 it is important to have random and uniform points distributions for each state variable. For these tasks phase and delay plots are used. The plottings also give visual results of "long run", dynamical behavior and chaotic attractors in each phase and time delay.

Thus we need to verify how a parameter different from the "1" influences to the chaotic behavior.

Phase plot (space) is a space in which all possible states (dimensions) of a system are represented at projectory $(x^i_n \; x^j_n)$, with each possible state of the system corresponding to one unique point in the phase space [13].

The Lozi 2 dimensional system ($z_1$ and $z_2$) is recognizable due to its lozenges after plotting where the density is lower and the system trajectories fall in less frequently, with lower probability (fig. 2-A).

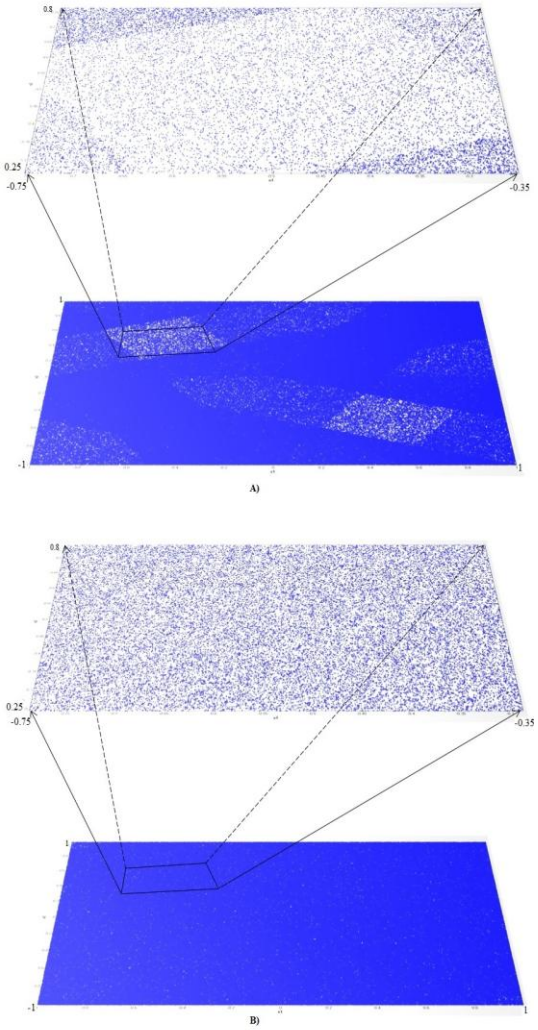


**Figure 2. A) Lozi system phase space (x1,x2); B) Modified Lozi system plotting (x1,x2) where a= 0.1**

The lower probability is obviously a drawback because it does not permit an uniform distribution, required for a good PRNG. To plot ( $x_1, x_2$ ) $3\times10^6$ points have been taken and the initial $2\times10^6$ points were cut off as transients.

It was noticed that the lozenges have been removed from the modified Lozi system ( $z_1'$ ) where a= 0.1 (fig. 2-B). Therefore there are no more regions with lower density in the phase plane. The same plotting parameters were taken to analyze $z_1'$ system.

After $10^6$ iterations the new system exhibits very few scattered empty points on the plane that implies flat distribution and chaotic behavior and the lozenges with lower density have been removed.

Delay plot (recurrence plot) is very close to the phase space but is used only for one dimension of the system with cartography of chaotic attractor with time delay $(x_n^i \;\; x_{n+1}^i)$, where $k \in [n+1; signal \;\; samples \;\; length]$.

To plot $3\times10^5$ points have been taken and the initial $2\times10^5$ points were cut off as transients for ( $x_n^1 \;\; x_{n+1}^1$ ) and the same value of points for ( $x_n^2 \;\; x_{n+1}^2$ ) (3-A).

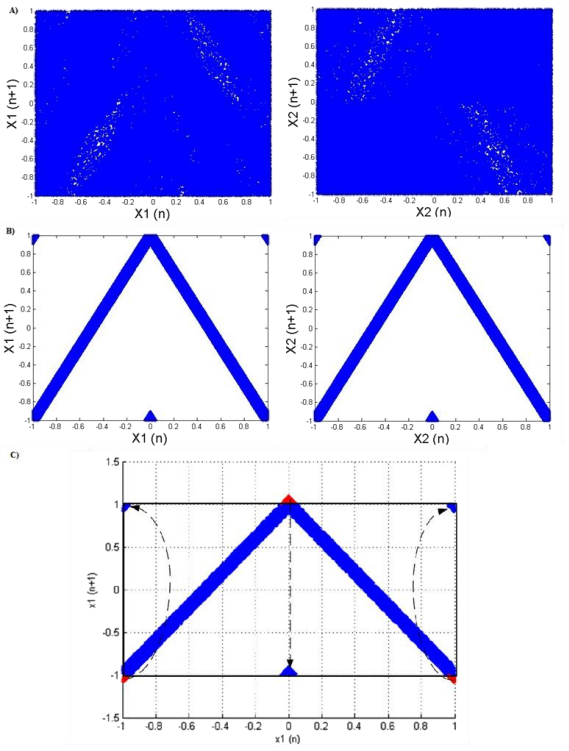


**Figure 3. A) Standart Lozi ploting at time delay B) System with a=0.1 plotting at time delay C) Returns points to the plain**

As we can see for Lozi system results are sufficiently good but there are regions where points fall down less frequently. The situation is similar to that of the phase plot so it is difficult to predict the system behavior. In ideal conditions the points are uniformly distributed everywhere in the plotting.

Now we verify long run of the system (2) by delay plotting where a=0.1 using the same conditions (fig. 3-B)

In the fig. 3-B we can see that the system is periodic and is predictable even if other tests demonstrate perfect randomness. We obtained the graph of tent map:

$$f_s \equiv T_s(x) = 1 - s|x|$$

This graph can be explained: small *a* parameter is reducing the part μ of the system (2) that makes points homogeneously distributed. On the unfolded torus graph is tent map but because some points were going out and to be returned to the plain by equation (3) there are points at the top left and right and bottom center as well, (fig. 3-C) .

Consequently to achieve uniform distribution in phase and delay plots, *a* parameter needs to be closer to 1(fig.4-A).

Another advantage of such modification is the long term behavior of the output systems $z_1$ and $z_1'$ (where a=1 and a = 0.99) whose trajectories don't converge to each other (fig.4-B). The interval from $3\times10^5$ to $3{,}001\times10^5$ iterations has been taken for instance to plot sequences.

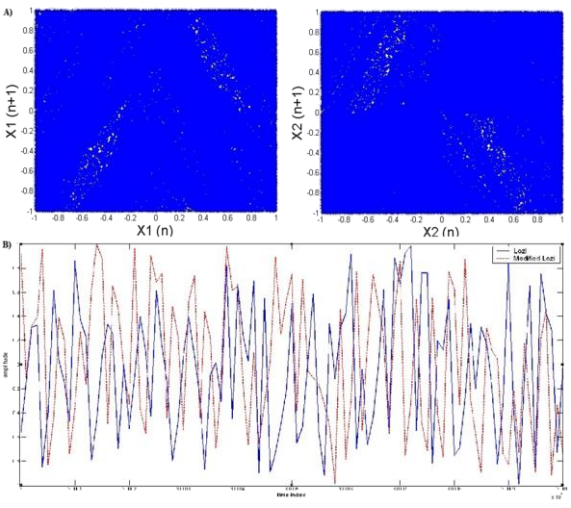


**Figure 4. A) System with a=0.99 ploting at time delay B) Trajectories of the Lozi and the modified Lozi systems don't converge to each other**

To verify more precisely randomness, statistical NIST tests and largest Lyapunov exponent have been used.

For the analysis two systems Lozi – ( $Z_1$ ) and modified Lozi – ( $Z_1'$ ) with parameter $a$=1 for the first and $a = 0.99$ for the second system have been compared while other parameters have been kept the same: $p$=2 (two-dimensional system) $e_1 = 10 \times 10^{-10}$, $e_2 = 2e_1$, $x_0$ is a random value (fig. 5).

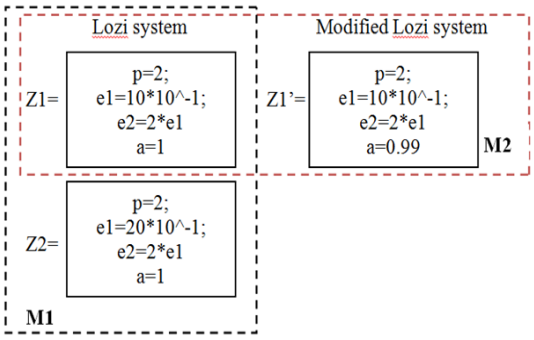


**Figure 5. Trasmitter parameters**

Thus the appropriateness of adding switched parameter $a$ to Lozi system is demonstrated and although modeled by deterministic map, the analyzed chaotic generator with new parameter exhibits excellent random properties.

## 5. Randomness tests for switched encrypting model based on modified lozi system

Randomness sequences statistical properties are displayed as graphical dependencies in appearance that drive conclusions about the sequence properties. This group consists of different set tests such as a histogram of distribution, autocorrelation function, cross correlation function, distribution of elements on the plane that are applied to analyze M2. M2 is the switched chaotic model (fig.1-C) where $Z_1$ and $Z_1'$ generators are used (fig. 5).

Autocorrelation function is described by equation (3) and is used as a qualitative tool for checking randomness. The random sequence has autocorrelations near zero for any and all time-lag. If one or more of the autocorrelations strongly deviate from zero, it indicates non-randomness.

$$R_X(j) = \frac{1}{N} \sum_{i=1}^{N} x_i x_{i+j} \quad (3)$$

The cross correlation function (4) however measures the dependence of the values of one signal $x_1$ of $Z_1$ generator on another signal $x_1'$ of $Z_1'$ generator.

$$R_{x1x2}(j) = \frac{1}{N} \sum_{i=1}^{N} x1_i \, x2_{i+j} \quad (4)$$

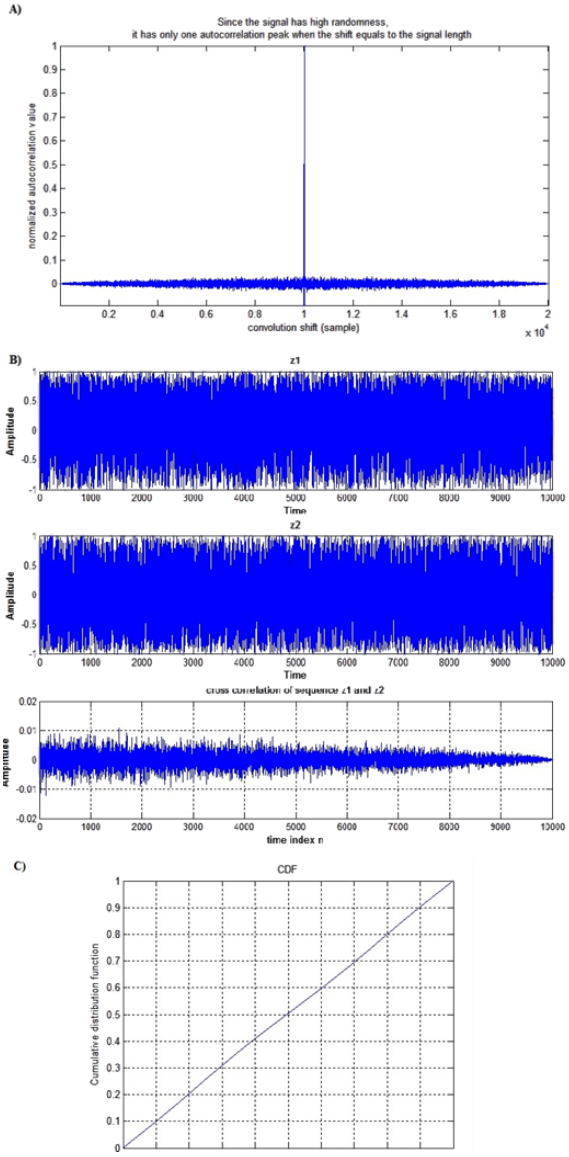


**Figure 6. A) Autocorrelation Cumulative B) Cross correlation C) distribution function (cdf), of the output of M2 (Z1-Z1')**

Uniform distribution guarantees unpredictability and is used to demonstrate randomness and suitability to cryptography. Cumulative distribution function has been chosen as being more informative than the histogram. In the random case x is uniformly distributed on the interval. Distribution histograms allow to estimate samples partition in the

studied sequence, and to determine the frequency of occurrence of a specific distribution value. For the random sequences the frequency character should be about the same. It is demonstrated in fig.6-C that M2 output sequence propagation is proportionally distributed in the interval [-1 1] where F(y) = number of output samples <= y / total number of output samples and this for all values in the output vector Y.

Iterating M2 from 500 000 to 1000 000 exhibits the following excellent features:

Minimum value: -1.0
Maximum value: 1.0
Sample mean: -1.7167e-04
Sample median (50th percentile): -9.9044e-04
Sample standard deviation: 0.5739

The modified Lozi system with new parameter has sufficiently good results: high complexity; auto-correlation (fig. 6-A) and cross-correlation (fig. 6-B) near to zero, normal distribution (fig. 6-C), balance on {-1, 1}. Thus it seems that sequences behave randomly, however, additional tests have to be carried out.

## 6. Two models comparison

Two switched encryption models based on Lozi and modified Lozi systems have been compared. For the first model M1 we take two generators $Z_1$ and $Z_2$ with different *e*-value (fig. 5) while the other parameters are the same: $p=2$ (two-dimensional systems), $x_0$ is randomly chosen. For the second model M2 we take two generators $Z_1$ and $Z_1'$ (fig. 5).

Each of the models encrypts 4 million message bits. To generate the test message, "Bernoulli Binary Generator" block of the Simulink with 0.5 probability of a zero has been used. The initial 1 mln points were cut off as transients out of 4 mln.

NIST requires binary form values hence for efficient parsing randomness we need to make binarization of the sequences according to IEEE-754 standard for 32 bit form.

64 bit binarization has not been used because $x_i = [-1 \quad 1]$, so that mantisa in binary form for integer part is the same and takes 11 bits information that are non-changeable and it leads to faulty verification for randomness.

31 bits for the decimal part and 1 bit for the sign according to IEEE-754 standard [14] for 32 bit were taken. The Matlab function quantizer([32,31]) for reservation 32 cells is used, where the first bit for the sign has been kept. Consequently function num2bin(q,data) makes binarization, where q – 32 'cells' and data – value which we want to binarieze. For example:

data = -0.4893
bin = 11000001010111101001111000011011
data = 0.8087
bin = 01100111100000110111101101001010

Where first bit is 0 when 'data'-value is positive and 1 when – negative. After binarization of the tested systems, NIST tests have been applied.

NIST statistical tests have been used as a tool to verify sequences produced by generator for randomness. For each test a conclusion is drawn about acceptance or refusal. Each of the tests is based on calculation value test statistic that is data function. This statistics takes weighted P-value which determines if the sequence is random.

The NIST package includes 15 statistical tests, the aim of which is the estimation of randomness measure for binary sequences: Frequency, BlockFrequency, CumulativeSums, Runs, LongestRun, Rank, FFT, NonOverlappingTemplate, OverlappingTemplate, Universal, ApproximateEntropy, RandomExcursions, Serial, LinearComplexity [5].

**TABLE 1. TWO MODELS COMPARISATION**

| Test Name | M1 | M2 |
|---|---|---|
| Frequency | 100 /100 | 98/100 |
| BlockFrequency | 98 /100 | 98/100 |
| CumulativeSums | 100 /100 | 99/100 |
| Runs | 99 /100 | 100/100 |
| LongestRun | 97/100 | 99/100 |
| Rank | 99/100 | 100/100 |
| FFT | 99/100 | 100/100 |
| NonOverlappingTemplate | 99/100 | 100/100 |
| OverlappingTemplate | 98/100 | 99/100 |
| Universal | 98 /100 | 99/100 |
| ApproximateEntropy | 99 /100 | 100/100 |
| RandomExcursions | 63/63 | 65/65 |
| RandomExcursions Variant | 63/63 | 63/64 |
| Serial | 98/100 | 99/100 |
| LinearComplexity | 96/100 | 98/100 |
| Time executing – 4mln bits | 2.9866e+04 | 2.1755e+04 |

As seen in the table (1) the results of the two systems are different, that means that chaotic behavior has changed and we succeeded to obtain new sequences while maintaining randomness, what was our aim. The performances of the switched M2( $Z_1$ - $Z_1'$ ) model have been studied for autocorrelations, cross-correlations, NIST tests and Lyapunov exponents.

Speed working is an important part of tests. After simulation using MATLAB, on Intel Core i7 Processor 1.6 GHz encryption of one Byte M2 consumes 0.16 ms/Byte instead of 0.165 of the M1 that is sensible for a big data transmission. Proposed

 

modification in generator meets the real-time encryption requirements and synchronization time for chaotic switching model can be compensated in such a way.

## 7. Results and future work to be undertaken

The proposed transformation in the Lozi system allows us to switch a parameter (depending on the bit of a message) to receive quickly splitting chaotic carrier trajectories and preserve randomness. The speed of execution by classical switched independent chaotic two generators (M1) is worse. Encrypting time for 400000 bit information is 2.9866e+04 matlab's time units, for the switched M1 model between two generators and 2.1755e+04 for the proposed model M2 with switched parameter.

We received new chaotic behavior that successfully passed all the tests: autocorrelations, cross-correlations, NIST tests and LLE.

For further work observer need to be designed for the decryption and to increase model security as well.

## 8. Summary

The switched chaos-based encryption model was achieved by using Lozi chaos system with adding switched parameter *a* depending on 0/1 bit of the message. The modified Lozi system was verified for randomness by auto-correlation, cross-correlation, and distribution. It successfully passed NIST tests, and largest Lyapunov exponent has been increased showing strong chaotic behavior. The execution speed has been increased. The proposed approach based on a chaotic switching scheme with structurally identical generators with parameter *a* offers to have larger encryption keys and allows in future research to make different modifications to improve security and robustness.

## 9. References

[1] F.Lau, C.Tse, "Chaos-based digital communication systems" (book) Hong Kong, China, Springer, Jun 4, 2003. - 228 p.

[2] Ali-Pacha, N. Hadj-Said, A. M'Hamed, A. Belghoraf, "Lorenz's Attractor Applied to the Stream Cipher (Ali-Pacha Generator)", Chaos, Solitons & Fractals - 2007, Volume 33/5, pp. 1762-1766

[3] Kazuyuki A., "Chaos and Its Applications", IUTAM Symposium on 50 Years of Chaos: Applied and Theoretical (2012), pp. 199-203

[4] National Institute of Standard and Technology "Random Number Generation and Testing", available at http://csrc.nist.gov/rng/ (8 December 2013).

[5] A.A. Koronovskii, O.I. Moskalenko, A.E. Hramov, "On the use of chaotic synchronization for secure communication", phisical sciences journal 2009 (in russian).

[6] En Li, Min Wu, Yonghua Xiong, "Design and application of encryption algorithm based on double chaos map", Application Research of Computers, 2009 (4), pp. 1512-1514.

[7] Yang T, Yang LB, Yang CM. Breaking chaotic switching using generalized synchronization: examples. IEEE Trans Circuits Syst I, 1998;45:1062.

[8] Andrew D., P. Jose, 1999. "Chaotic Generation OF PN Sequences: AVLSI Implementation", proceedings of the 1999 IEEE International Symposium on Circuits and Systems, pp. 454-457.

[9] R. Lozi , E Cherrier "Noise-resisting ciphering based on a chaotic multi-stream pseudo-random number generator", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, 1, Abu Dhabi, United Arab Emirates

[10] A. Espinel, I. Taralova, R. Lozi "New alternate ring-coupled function for random number generation", Journal of Nonlinear Systems and Applications 2012

[11] L. D. Iasemidis, J. C. Sackellares, H. P. Zaveri, & W. J. Williams, "Phase space topography and the Lyapunov exponent of electrocorticograms in partial seizures", Brain Topography, 2 (1990), pp. 187 – 201

[12] R. Hegger, H. Kantz, T. Schreiber, "Practical implementation of nonlinear time series methods: The TISEAN package", CHAOS, 9, 413, (1999)

[13] Nolte, D. D. (2010). "The tangled tale of phase space", Physics Today 63 (4), pp. 33–38

[14] IEEE 754-2008. IEEE 754-2008 Standard for Floating-Point Arithmetic. August 2008, 70 p.

 