*Chaotic Modeling and Simulation (CMSIM)* **2: 117-128, 2015**

# Computer modeling of information properties of deterministic chaos

Mykola Kushnir, Sergii Galiuk, Volodymyr Rusyn, Grygorii Kosovan, Dmytro Vovchuk

Physical, Technical and Computer Science Institute of Chernivtsi National University, Chernivtsi, Ukraine
(E-mail: kushnirnick@gmail.com)

**Abstract.** Since mathematical models describing the work of transmitting-receiving units of modern chaotic information systems have become more complex, modeling of information properties of deterministic chaos is becoming more topical. The paper presents the results of a wide range of works related to the modeling of dynamic chaos usage in modern telecommunication systems - from generating chaotic sequences to their application for information security and as the actual information media.
**Keywords:** Deterministic chaos, chaotic system, computer modeling, information properties.

## 1 Introduction

Nowadays, there is a rapid development of both new methods of information transmission and security, and new means of processing analog and digital information flows that come in opened or closed state. Deterministic chaos is one of the new elements which is recently started to be frequently used in modern communication systems Banerjee et al.[1]. In short, this phenomenon is complex nonperiodic oscillations that occur under certain conditions (parameters) and are the inner nature of the so-called chaotic dynamical systems Cvitanovic et al.[2]. This paper presents generalized complex results on the dynamic chaos usage in modern communication systems, which are carried out in the laboratory for the study of chaotic processes in radio-engineering of the Physical, Technical and Computer Science Institute of Chernivtsi National University.

The paper has the following structure. In the second section the relation between the Lyapunov exponents and information properties of chaotic oscillations is analyzed. The third section is devoted to the modeling of hyperchaotic systems in the environment LabView. In the fourth section some topical issues of the dynamic chaos usage for information security are discussed, namely the formation of pseudorandom generators based on two chaotic systems. The fifth section presents the studies of models of information systems using deterministic chaos and also some obtained numerical characteristics.

Received: 28 July 2014 / Accepted: 25 November 2014

ISSN 2241-0503

## 2 Lyapunov exponents and information properties of chaotic signals

For practical use of chaotic signals it is necessary to use criteria of signals complexity. The characteristics of chaotic signals, allowing them to be compared include: fractal dimensions (correlation dimension, information dimension), Fourier spectrum, Poincare section, Lyapunov exponents, topological entropy, etc Francis C. Moon[3]. Fractal dimension of the attractor allow to evaluate the metric complexity of its trajectories in phase space. Fractal characteristics of chaotic attractors are invariant to the time scale of chaotic systems. The information properties of signals are important for communication, cryptography and other applications. Visual image of a dynamic system is its attractor.

Informational properties of chaotic oscillations can be estimated using the Lyapunov exponents. In the theory of dynamical systems the Lyapunov exponent is a quantitative measure of the exponential divergence of initially close trajectories. If the initial distance between the trajectories is $d_0$ then at time $t$ the average distance between them will be $d(t) = d_0 e^{\lambda t}$, where $\lambda$ – Lyapunov exponent. In terms of information theory, the largest Lyapunov exponent is numerically equal to the average information created by a dynamic system. Next, we show that the Lyapunov exponents are dependent on the time scale of the dynamic system.

Consider the Rossler system, described by the system of three differential equations Rossler[4]:

$$\begin{cases} \dfrac{dx}{dt} = -(y+z), \\ \dfrac{dy}{dt} = x - ay, \\ \dfrac{dz}{dt} = b + z(x-c), \end{cases} \tag{2.1}$$

where $x$, $y$, $z$ – state variables, $a$ = 0.15, $b$ = 0.2, $c$ = 10 – system parameters for which there is a chaotic regime.

The values of the Lyapunov exponents of the system (2.1) are as follows: $\lambda_1$ = 0.09, $\lambda_2 = \lambda_3$ = -9.82. We will change time scale in the system (2.1) by replacing $t = kt'$, where $k > 0$, and obtain a system (2.2):

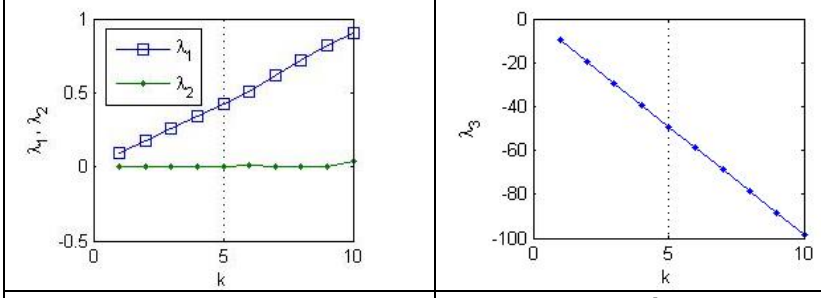
$$\begin{cases} \dfrac{dx}{dt} = -k(y+z), \\ \dfrac{dy}{dt} = k(x-ay), \\ \dfrac{dz}{dt} = k(b+z(x-c)), \end{cases} \tag{2.2}$$

Systems (2.1) and (2.2) have the same chaotic attractors and fractal dimensions, but the Lyapunov exponents of the system (2.2) are linearly dependent on the parameter $k$ as shown in Figure 2.1.

By varying the time scale of chaotic systems (2.2) by changing the parameter $k$ it is possible to control the speed of generating information. This is a practical method of information properties management of dynamical systems. At the same time, the change of time scale of chaotic systems is equivalent to the change of width of the oscillations spectrum in $k$ times. This means that the value of the senior Lyapunov exponent and the width of the signal spectrum are interconnected. For example, consider two chaotic flow systems – the Rossler system (2.1) and the Lorenz system Lorenz[5]:

$$\begin{cases} \dot{x} = \sigma(y - a), \\ \dot{y} = rx - y - xz, \\ \dot{z} = xy - bz, \end{cases} \tag{2.3}$$

where $\sigma$ = 10, $r$ = 28, $b$ = 8/3 – system parameters.




*a* *b*

Fig. 2.1. Dependence of the Lyapunov exponent on parameter $k$: $\lambda_1$, $\lambda_2$ – *a*; $\lambda_3$ – *b*.

For the Lorenz system for the given parameters the values of the Lyapunov exponents are as follow: $\lambda_1$ = -9.82, $\lambda_2$ = 0.9, $\lambda_3$ = -14.57. The value of the largest Lyapunov exponent of the Lorenz system is greater than the largest Lyapunov exponent of the Rossler system in 10 times. As shown in Figure 2.2 and Figure 2.3 the signal spectrum of the Lorenz system is more complex and broader than in Rossler system.

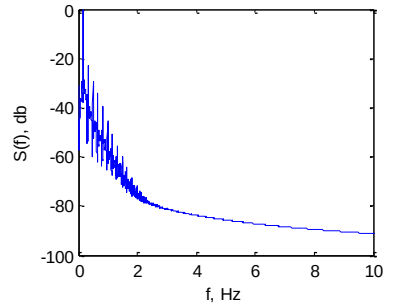



Fig. 2.2. Normalized spectrum of the variable $x$ of the Rossler system (2.1)

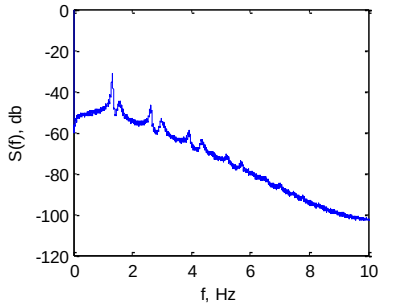



Fig. 2.3. Normalized spectrum of the variable $z$ of the Lorenz system (2.3)

In general, the signal complexity is a composit concept and includes spectral, information and metric data. Therefore, we can conclude that the Lyapunov exponent characterizes the signal complexity in terms of its information properties, but contains little information regarding the complexity of the metric structure of the signal. This means that it is incorrect to compare in general the signals complexity of continuous dynamic systems using only the value of the largest Lyapunov exponent.

## 3 Modeling of information properties of the hyper-chaotic Lorenz system

Hyper-chaotic Lorenz system is described by equations:

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = bx + y - xz - w, \\ \dot{z} = xy - cz, \\ \dot{w} = kyz, \end{cases} \tag{3.1}$$

where $a, b, c$ – system parameters, $x, y, z$ – initial conditions, $k$ – constant that determines the attractor, which in some senses can be chaotic, and in particular – controlled Tiegang Gao et al.[6].

For modeling of information properties of the hyper-chaotic Lorenz system we used LabView programming environment [7].

Figure 3.1 shows the block scheme that implements of hyper-chaotic Lorenz system. The main functional part is a formula node, in which would include the equation (3.1). In the input formula node fed values of system parameters ( $a, b, c$ ) and the value of the initial conditions ( $x, y, z$ ). At the output assigned equations (3.1). Also, the output is an opportunity to demonstrate the solution of equations in three dimensions.

When changing the system parameters and initial conditions we can be analyzed in detail and investigate the behavior of a hyper-chaotic Lorenz system, which in many cases is a basic element of the functional blocks of chaotic secure communication systems.

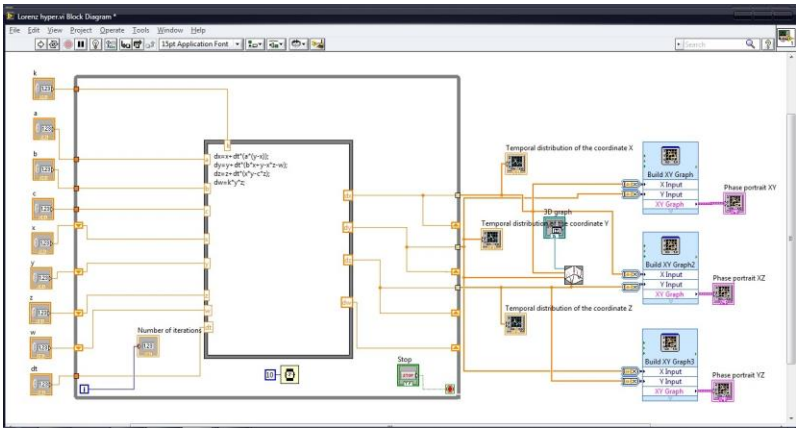



Fig. 3.1. Block scheme of hyper-chaotic Lorenz system

Figure 3.2 shows the software interface which shows these information modeling properties as temporal distributions of the values of the coordinates X, Y, Z, three-dimensional map of hyper-chaotic attractor and phase portraits in the planes XY, XZ, i YZ, when the number of iterations $N = 5000$, the system parameters $a = 10$, $b = 28$, $c = 8/3$, $k = 0{,}1$, and initial conditions $x = y = z = 1$.

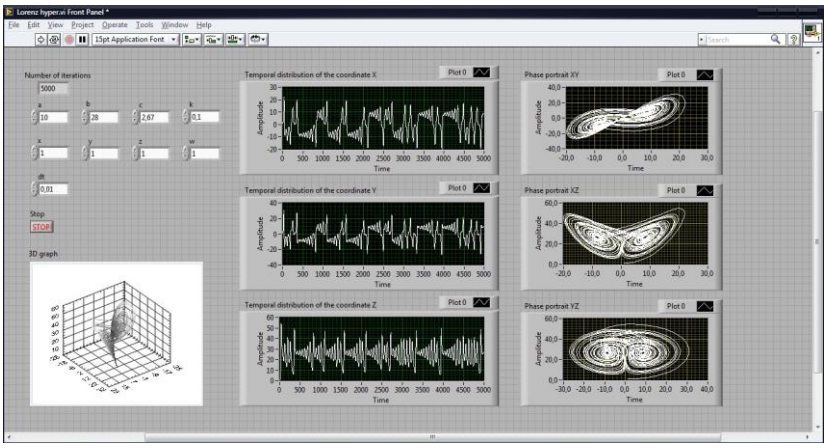



Fig. 3.2. Software interface which shows modeling of information properties

Figure 3.3 shows the spectral analysis of chaotic coordinates X, Y, Z with the number of iterations $N = 5000$ which was conducted using fast Fourier transform. The value 0.01 corresponds to 100 Hz.

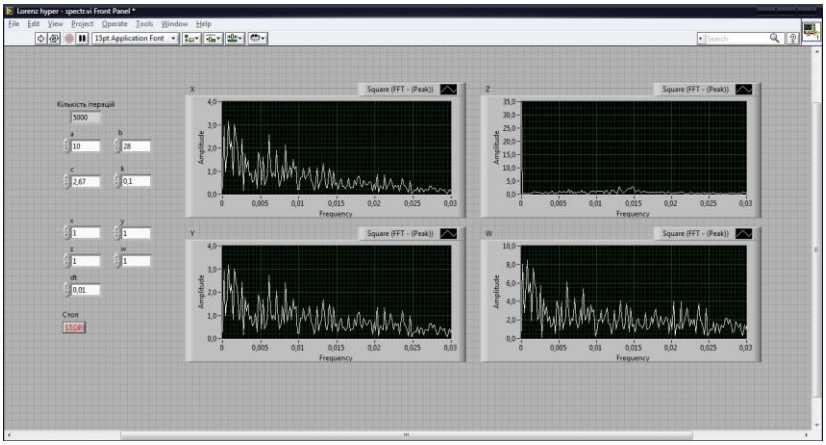



Fig. 3.3. Fourier spectral analysis when the number of iterations $N = 5000$

Developed block diagram in LabView programming environment allows the program to explore the hyper-chaotic Lorenz system.

## 4 The use of dynamic chaotic systems in cryptography

Since with the development of information technology there is as well the development of means of data interception, there is a need in the development of new algorithms of information encryption. Dynamic systems are sensitive to the initial conditions and control parameters, which makes them good candidates for use in the development of encryption algorithms.

We have proposed a method of generating pseudorandom sequence of bits using two dynamic chaotic systems and operations XOR Shahtarin et al.[8]. The first dynamic system – the Lorenz system described by equation (4.1), the second – a logistic mapping described by equation (4.2).

$$\begin{cases} \dot{x} = -a(x - y), \\ \dot{y} = cx - y - xz, \\ \dot{z} = bz + xy, \end{cases} \qquad (4.1)$$

where $x$, $y$, $z$ – dynamic variables; $a$, $b$, $c$ – parameters of the Lorenz system, which usually possess the values $a = 10$, $b = 8/3$, $c = 28$.

$$\upsilon_{n+1} = r\upsilon_n(1-\upsilon_n), \qquad (4.2)$$

where $v_n$ and $r$ – system variable and system parameter respectively, $n$ – iteration number. The system parameter $r$ is a significant part of the equation and if the values $3.57 < r < 4$ the system is characterized by chaotic behavior.

Both dynamic systems were used to generate values of dynamic variables Arvind et al.[9]. The values of dynamic variables $x$, $y$ and $z$ of the Lorenz system were compared with the generated value $\nu$ of logistic mapping. If the value of Lorenz system variable was larger than the value of the variable of logistic mapping, a decision was made that the generated logical «1» otherwise logical «0». Thus three sequences of bits are being generated $k_1$, $k_2$ and $k_3$ that

are joined together using XOR operation thus forming total pseudorandom sequence of bits. Then the obtained sequence can be used for information encryption.

However, for the correct operation of such generator it is necessary to coordinate the range of output values of the Lorenz system with the range of output values of logistic mapping. This is done by mapping the obtained value of the variable within the interval (0;1).

We have performed simulation of the proposed generator operation in the environment LabView, block diagram of the generator is shown in Figure 4.1. Simulation has shown that the proposed generator can be easily implemented by software and is quite quick Kosovan[10].

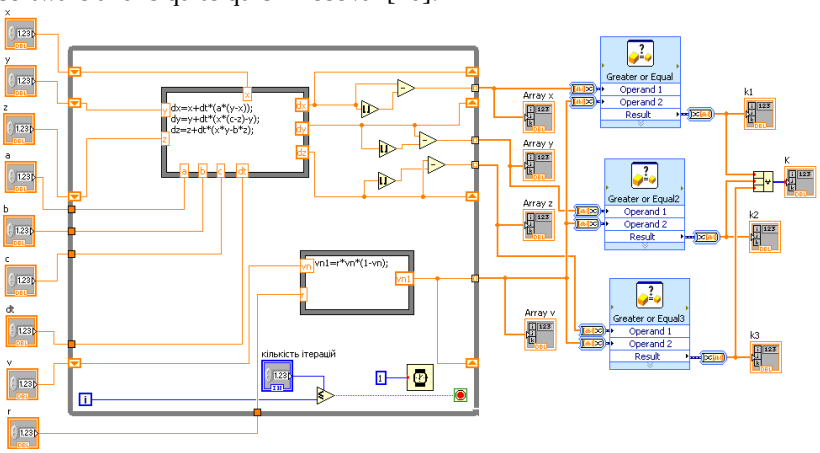



Fig. 4.1. Block diagram of the generator based on two dynamic systems

Also, we have implemented the proposed generator in the programming language Delphi 7 an external view of the program is shown in Figure 4.2.

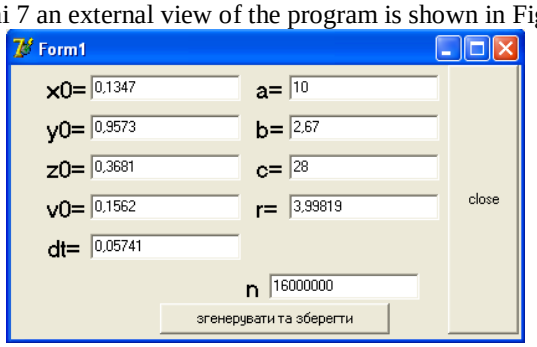



Fig. 4.2. An external view of implementation program of the bit sequences generator, where $x_0$, $y_0$, $z_0$ and $v_0$ – initial conditions of dynamic systems; $a$, $b$, $c$ and $r$ – control parameters; $dt$ – integration step; $n$ – the length of generated sequence.

To check whether the proposed generator has the properties of a pseudo randomness, the sequence of bits with the length of 16000000 bits was generated. The sequence generation was performed when the values of initial conditions were the following: for the Lorenz system $x_0 = 0.1347$, $y_0 = 0.9573$, $z_0 = 0.3681$, $a = 10$, $b = 2.67$, $c = 28$ and integration step $dt = 0.05741$ for cubic mapping $v_0 = 0.1562$ and $r = 3.9979$. In this algorithm the integration step $dt$ and control parameter $r$ play a significant role in keys forming, so it is necessary to carefully select their values to be able to obtain the generated pseudorandom sequence of bits of large length.
The obtained sequence was tested using a set of statistical tests NIST STS-1.6. 15 of 16 tests passed.
On the basis of obtained results we can conclude that the generated sequence is really pseudorandom and the proposed generator can be used in the development of algorithms of information encryption. Also the proposed generator has a large number of keys (initial conditions and parameters), namely 9 of which 6 can change their values over the sufficiently wide range. If you set keys with an accuracy of 5 decimal places a number of their possible combinations will be approximately $10^{35}$. Such a large number of keys complicates their selection and makes brute-force attack more complex and costly.

## 5 The research of the possibility of information recovery, its hiding and noise immunity in information systems using deterministic chaos

Nowadays, the development of digital systems of hidden communication using chaotic signals is a topical issue. Numerous works offer analog communication systems that use the synchronization of transmitter and receiver for data recovery Politansky et al., Eliyashiv et al.[11-12]. The research has found that such systems possess low noise immunity caused by high sensitivity of chaotic synchronization to the noises in the communication channel and by the parameters detuning of drive and response generators. The use of digital systems provides both the rise of noise immunity level of data transmission process, compared to the analog ones, and the possibility of encoding Bollt, Lai [13] and cryptographic security methods Baptista[14] application.
The most widely used scheme for hidden digital communication is the chaotic switching scheme using full synchronization phenomenon Koronovskii[15]. Among the systems of hidden transmission of analog information the most widely used is the circuit with the use of chaotic masking Downes, Ivanyuk et al.[16-17] that is analytically defined by the system of differential equations (5.1). The principal of system operation is as follows. One of the output chaotic oscillations of the generator $x(t)$ is summed up with an analog data signal $m(t)$ followed by transmission to channel. Security of the data transmission process through the channel is ensured by complete overlap of the data signal spectrum by chaotic oscillation spectrum. The receiver contains one chaotic generator

*u(t)*, identical to transmitter generator. Recovered signal can be obtained after passing through subtractor as the difference between the receiver input signal and the response generator output signal. The control parameters variety of drive and response generators and the presence of noises in communication channel results in arising of synchronization error that equals the error of data signal recovery. Desynchronization of transmitter and receiver generators eliminates the possibility of data recovery, transmitted through the channel. Besides, it is necessary to ensure the ratio signal/noise no less than 35 dB for accurate data recovery, which is its principal disadvantage Vovchuk et al.[18].

$$\begin{cases} \dot{x} = \alpha(y - x - f(x)), \\ \dot{y} = x - y + z, \\ \dot{z} = -\beta y, \end{cases} \quad \begin{cases} \dot{u} = \alpha(v - u - f(v)) + e(x - u), \\ \dot{v} = x - v + w, \\ \dot{w} = -\beta v, \end{cases} \tag{5.1}$$

where *x*, *y*, *z*, *u*, *v*, *w* – dynamic variables; *e* – coupling coefficient.

When using the circuit of chaotic masking in digital systems of data transmission, the hiding of transmission process through the channel will be low as in the intervals, that are equal to the duration of data bit transmission, a strong constant component will take place. In order to eliminate this defect we offer a modification of analog circuit of chaotic masking for digital communication [18]. In contrast to the circuits of analog data transmission it contains a subsidiary generator *G*, the signal of which is modulated by digital data signal and added to the chaotic signal. The modulation is carried out with the aid of a key which is turned on or off depending on the value of data bit. The implementation of preliminary modulation and ensuring the identity of statistic and spectral characteristics of signals generated by the generator *G* and the masking oscillation *x(t)* enables to match the parameters of carrying and chaotic signals. Both harmonic and chaotic signal can be used as a signal *G(t)* [18]. The receiver model remained unchanged. Mathematic model differ only by the presence another component in the fifth equation that describes the type of modulated carrier oscillation, namely $m(t)A\sin(2\pi ft)$ or $m(t)y(t)$, when using the harmonic or chaotic oscillation, respectively.

If the chaotic oscillation is used as carrier then it is sufficient for hidden communication that its spectrum is completely offset by masking oscillation one. There is other situation using harmonic signal as carrier. In this case, the hiding in the channel depends on its frequency and amplitude values.

The harmonic signal hiding decreases with increasing the value of its amplitude. But the decrease in harmonic signal amplitude leads to the decrease in power of desynchronization signal of drive and response systems and consequently to the decrease in noise immunity of information transmission in general. Thus, for reliable operation of the system with chaotic masking it is necessary to choose a compromise between the chaotic and harmonic signal values.

In the modeling process the amplitude *A* and frequency *f* were varied. The curves family (Figure 5.1) of a dependence $\frac{P_{desyn}}{P_{ms}}(\frac{P_{hs}}{P_{ms}})$, where $P_{desyn} = P_{S(t)} - P_{u(t)}$ - power of a desynchronization signal, $P_{S(t)}$ - signal power

in the channel, $P_{u(t)}$ - power of response generator output signal, $P_{hs}$ - harmonic signal power, $P_{ms}$ - masking signal power. The figure analysis showed that increasing of harmonic signal amplitude leads to increase in value $P_{desyn}$. The dependence is linear when the values *f* are up to 1 kHz, while $P_{desyn}$ does not exceed 20 % of $P_{ms}$. An increase *f* leads to the complication of dependence. When *f* are increasing closer to the upper frequency spectrum of a chaotic signal $f_7$ = 3,2 kHz та $\frac{P_{hs}}{P_{ms}} > 0.04$, the value $P_{desyn}$ practically does not depend on *A* and has 80-90 % of $P_{ms}$. If *f* goes beyond the chaotic oscillation spectrum, the dependence $\frac{P_{desyn}}{P_{ms}}(\frac{P_{hs}}{P_{ms}})$ gets more complicated and even when $\frac{P_{hs}}{P_{ms}} > 0.12$ the value $P_{desyn}$ increases significantly.

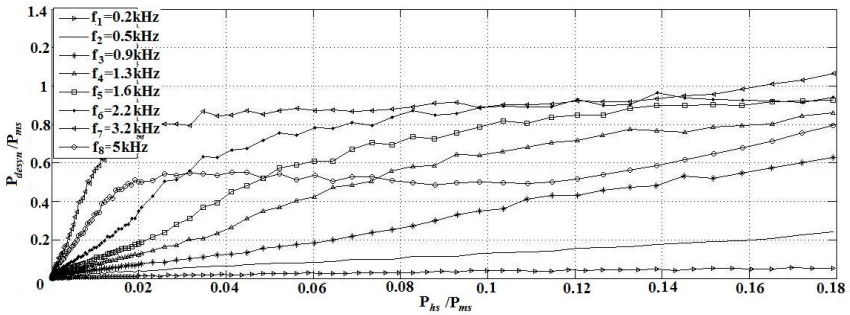



Fig. 5.1. The dependence of the normalized power of the desynchronization signal on the normalized power of the harmonic signal by changing the values of the amplitude and frequency of the harmonic signal

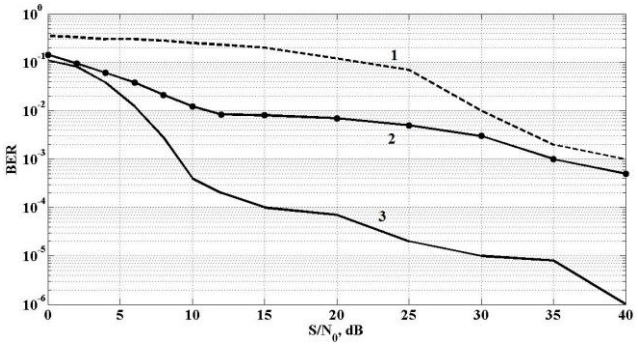



Fig. 5.2. Dependence of the probability of incorrect bits recovery on the value of signal/noise ratio in communication channel (1 – with harmonic oscillation used as a carrier signal; 2 –chaotic switching scheme; 3 – with chaotic oscillation used as a carrier signal)

Therefore, for the improvement of quality of information recovery it is reasonable to use the harmonic signal with a frequency close to the upper frequency of the chaotic signal. The obtained results can also be used for analog communication systems, where the harmonic oscillation is the information.
The dependence of error probability of the received data on the value of signal/noise ratio in communication channel is shown in Figure 5.2. The obtained results show that the system of data transmission based on the usage of harmonic oscillation as a carrier signal yields to the chaotic switching scheme by its noise immunity (Figure 5.2 - curve 1 and curve 2 respectively).
The system based on the usage of chaotic oscillation as a carrier signal is more resistant to noise impact in the channel (curve 3). The error probability of recovery when using the modified circuit with the ratio $S/N_0$ of the order 10 dB is $10^{-3}$, whereas its value constitutes $10^{-2}$ while using the chaotic switching scheme.

## Conclusions

The results given in this paper once again demonstrate the importance of the extensive use of deterministic chaos in modern secure communication systems - both as a basic component for information encryption and encoding and as the actual information carrier. Since the behavior of information systems models is being studied in the various software environments, then on our opinion the special attention in future researches should be focused on the analysis of pseudorandom properties of chaotic sequences and the ability to control the behavior of chaotic systems. Speaking about the choice of one or another software environment, we would advise to pay attention to the system LabView, which makes it possible to analyze both software and hardware solutions in a very wide circuit range (from analog circuits to FPGAs).

## References

1. Santo Banerjee, Mala Mitra, Lamberto Rondoni (Editors). Applications of Chaos and Nonlinear Dynamics in Engineering – Vol. 1 Springer-Verlag Berlin Heidelberg 2011, 358p.
2. P. Cvitanovic, R. Artuso, R. Mainieri, G. Tanner, G. Vattay. Chaos: Classical and Quantum I: Deterministic Chaos, ChaosBook.org version13, Dec 31 2009, printed January 9, 2010, 919p.
3. Francis C. Moon, Chaotic vibrations: An introduction for applied scientists and engineers, Wiley-Interscience, New York, 1987, 322 p.
4. O. E. Rossler, An equation for continuous chaos, Phys. Lett. A., 1976, Vol. 57, № 5, P. 397–398.
5. E.N. Lorenz Deterministic nonperiodic flow, J. Atmos. Sci. 1963, Vol. 20, № 2, P. 130–141.

6. Tiegang Gao, Guanrong Chen, Zengqiang Chen, Shijian Cang. The generation and circuit implementation of a new hyper-chaotic based upon Lorenz system. Physics Letters A 361, 2007.
7. Http://www.ni.com
8. B.N. Shahtarin, P.I. Kobylkina, Ju.A. Sidorkina, A.V. Kondrat'ev, S.V. Mitin. Generatory haoticheskih kolebanij , – M.: Gelios ARV, 2007. – 248 p.
9. T. Arvind, Chandana S. Nilavan and V. Prithviraj. New approach to information security through nonlinear dynamics and chaos. National Workshop on Cryptology. - Oct. 16-18. – 2003. - Chennai.
10. G. Kosovan, N. Kushnir, L. Politanskii. Simulation of algorithm for generating the encryption key information based on dynamical systems. Eastern-European Journal of Enterprise Technologies, 4/8 (64), 2013.
11. L. Politansky, S. Galiuk, M. Kushnir, R. Politansky. Osoblivosti sinhronizaciï haotichnih sistem (ogljad), Izdatel'stvo Fiziko–matematicheskoj literatury, Skladni sistemi i procesi, №2, pp. 3-29, 2011 (in Ukrainian).
12. Eliyashiv O.M., Galyuk S.D., Politanskii L.F., Kushnir N.Ya., Tanasyuk V.S. Continuous and pulse synchrozation of Chua oscillatiors, Tekhnologiya i Konstruirovanie v Elektronnoi Apparature, №3, 22 – 27, 2011 (in Ukrainian).
13. Bollt E., Y.-C. Lai Dynanics of coding in communicating whits chaos, Phys. Rev. E., Vol. – 58. - № 2. – P. 1724-1736, 1998.
14. Baptista M. S. Cryptography with chaos, Phys. Lett. A., Vol. 240. - № 1-2. - P. 50-54, 1998.
15. Koronovskii A., Moskalenko O., Hramov A. On the use of chaotic synchronization for secure communication, Uspekhi Fizicheskikh Nauk, 179, № 12, 1282-1310, 2009.
16. Ph. Downes. Secure communication using chaotic synchronization, SPIE, V. 2038. P. 227, 1993.
17. Ivanyuk P., Politansky L., Politansky R., Eliyashiv O. Chaotic masking of information signals using generator based on the Liu System, Tekhnologiya i Konstruirovanie v Elektronnoi Apparature, №3, 11-17, 2012 (in Ukrainian).
18. D. Vovchuk, S. Haliuk, L. Politanskii. Adaptation of the chaotic masking method for digital communication, Eastern-European Journal of Enterprise Technologies, № 2/4(62), pp. 50-55, 2013.