BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Tomul LXI (LXV), Fasc. 3, 2015
Secţia
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

# SECURE COMMUNICATION SYSTEM BASED ON ANALOG CHAOS MODULATION

BY

**CARMEN GRIGORAŞ[1,2] and VICTOR GRIGORAŞ[3,*]**

[1]”Gr. T. Popa” University of Medicine and Pharmacy of Iasi,
Faculty of Medical Bioengineering,
[2]Institute of Computer Science of the Romanian Academy - Iasi Branch,
[3]Technical University “Gheorghe Asachi” of Iaşi,
Faculty of Electronics, Telecommunications and Information Technology

Received: September 15, 2015
Accepted for publication: September 30, 2015

**Abstract.** This paper presents the design of a secure data transmission system, based on chaos synchronization and direct modulation. The proposed communication system is based on a simple analogue nonlinear emitter aiming at inexpensive implementation. We present the modified chaotic system, adapted for the purpose of synchronization and modulation, and analyze its nonlinear dynamics. The general setup of the data transmission system, conditions for correct synchronization, demodulation and error compensation are also analysed. Finally, possible applications in analogue and digital communication are suggested.

**Key words:** chaos synchronization; nonlinear dynamics; secure data transmission; nonlinear systems.

## 1. Introduction

Spread-spectrum communication using chaotic synchronization and modulation is an important domain of research in the last years. The idea is to develop a state observer for a nonlinear system performing chaotically as a synchronizing receiver and then modulate the information signal onto the chaotic carrier. The demodulation of the transmitted signal is performed with a supplementary circuit added to the synchronizing receiver. Both

[*] Corresponding author: *e-mail*: grigoras@etti.tuiasi.ro

synchronization and demodulation need to have access to the exact values of the emitter parameters, thus ensuring a supplementary level of security over the classic encryption. To verify the extra level of security the sensitivity to parameter mismatch between emitter and receiver must be tested, higher sensitivity leading to better security. But high sensitivity to the initial condition and parameter mismatch are related to unwanted channel noise and perturbation sensitivity, leading to noisy data recovery. Another type of error in data transmission based on chaotic modulation is linear distortion, of both amplitude and phase types. These must be analyzed and compensated in order to achieve good data recovery at the receiver end of the communication channel.

Our approach is based on a modified version of a previously reported chaotic system (Grigoraş & Grigoraş, 2015). The proposed system is simpler and faster than other reported chaotic generators using similar nonlinearities (Chua & Gui-Nian Lin, 1990; Elwakil & Kennedy, 2001; Li *et al.*, 2015), due to the use of fast comparators instead of diode or discrete transistor type switching elements. The synchronization structure used in our research is based on the system partitioning method, first introduced in (Carrol & Pecorra, 1991). The possibility of synchronization is analytically demonstrated including an input-output characterization of the resulting communication system. The resulting model is a linear dynamic system showing frequency limitations for the modulating signal. To increase the transmitted signal bandwidth, a feedforward equalizer is used, as first proposed by Grigoraş *et al.* (2009) and Grigoraş and Grigoraş (2010).

Section two presents the modified chaotic system, with added parameters to help developing a synchronizing receiver and better modelling of the circuit elements. The next section develops the synchronizing receiver and demonstrates its performance by means of the error dynamics method. By using a linear equalizer, the proposed setup frequency bandwidth is increased. Simulation results, confirming the theoretical results previously presented, are included in the fourth section. Short concluding remarks end our contribution.

## 2. The Modified Nonlinear System

The design of the emitter system starts from a previously reported chaotic circuit (Grigoraş & Grigoraş, 2015), which benefits from a simple structure, using only one comparator as a nonlinear element, leading to the possibility of inexpensive implementation:

$$\begin{cases} \mathrm{d}x/\mathrm{d}t = \omega y - z, \\ \mathrm{d}y/\mathrm{d}t = -\omega x + z, \\ \mathrm{d}z/\mathrm{d}t = -x - y - \omega z + \operatorname{sign}(x). \end{cases} \tag{1}$$

In order to adapt the system (1) to the goal of chaos synchronization and modulation, we introduce two slight modifications as follows:

a) to ensure the global asymptotic stability of the synchronizing receiver, we add a new term in the first equation, dependent on the *x* state variable;

b) to model the system closer to the electronic implementation, we replace the ideal nonlinear function, ‘sign(·)’, by the saturation type function, ‘sat(·)’, that takes into account the finite gain of the comparator, *G*:

$$\mathrm{sat}(u) = \begin{cases} 1 \quad \Leftrightarrow \quad u > 1/G, \\ Gu \quad \Leftrightarrow \quad |u| \le 1/G, \\ -1 \quad \Leftrightarrow \quad u < -1/G. \end{cases} \tag{2}$$

Taking into account these modifications, the state equations of the emitter system become:

$$\begin{cases} \mathrm{d}x/\mathrm{d}t = -ax + \omega y - z, \\ \mathrm{d}y/\mathrm{d}t = -\omega x + z, \\ \mathrm{d}z/\mathrm{d}t = -x - y - \omega z + \mathrm{sat}(x). \end{cases} \tag{3}$$

The modified nonlinear system preserves the dissipative nature of the initial one, as shown by calculating the divergence of the nonlinear state transition function:

$$\nabla \mathbf{f}(\mathbf{x}) = \frac{\partial f_1(\mathbf{x})}{\partial x} + \frac{\partial f_2(\mathbf{x})}{\partial y} + \frac{\partial f_3(\mathbf{x})}{\partial z} = -a - \omega \,. \tag{4}$$

For all positive values of *a* and *ω*, the divergence is negative, confirming the system disipativity:

$$\nabla \mathbf{f}(\mathbf{x}(t)) < 0 \quad \forall t > 0\,. \tag{5}$$

To verify the nonlinear dynamics of the modified system, (3), we analyzed its behavior, at the variation of the newly introduced coefficients, *a* and *G*, obtaining the bifurcation diagrams in Fig. 1. As can be noticed from the parametric analysis simulations, for all values of the parameter, *G*, larger than 80, the dynamic behavior of the nonlinear system remains roughly unchanged, maintaining the chaotic behavior of the initial system (1). On the contrary, the variation of the coefficient, *a*, exhibits a richness of dynamics, with periodic oscillations of periods 2, 3, 4 and 5, which show successive bifurcations towards regions of chaos, at the increase of the parameter value.

For adequate values of the system parameters, as identified on the bifurcation diagrams, we made in depth verifications of the dynamic behavior of the state variables. For instance, the phase portraits in Fig. 2 exemplify the case of periodic behavior, with period multiplication by a factor of three, obtained for *G* = 100 and *a* = 0.16, and the case of chaotic dynamics, obtained by modifying the value of ‘*a*’ to 0.22.

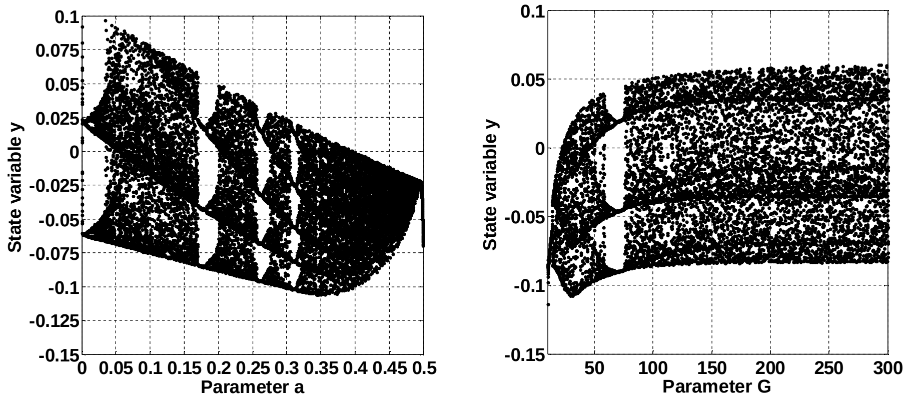

Fig. 1 – Bifurcation diagrams at the variation of parameter *a* (left) and *G* (right).

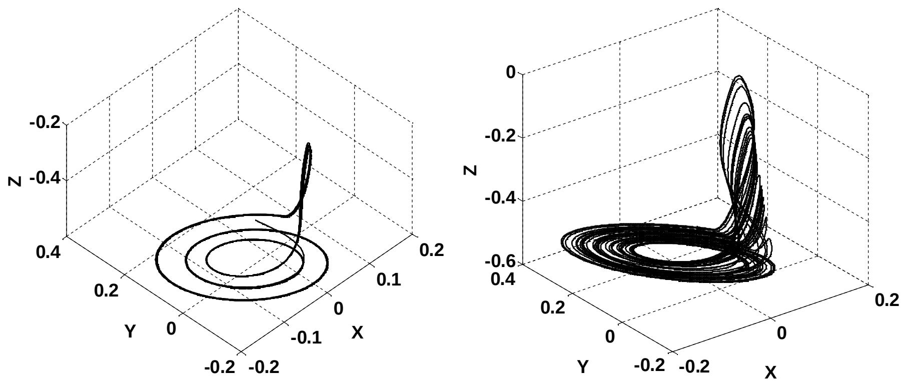

Fig. 2 – Phase portraits for periodic (left) and chaotic (right) behaviours.

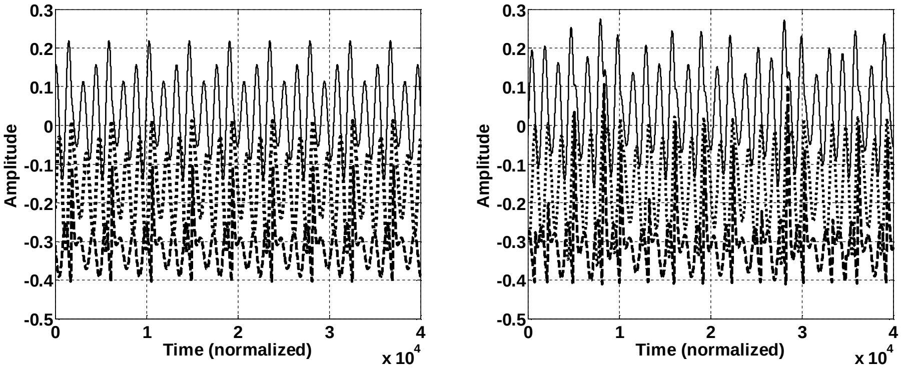

Fig. 3 – Time evolution of the state variables: *x* – thin continuous, *y* – dotted and *z* – thick dashed, for periodic (left) and chaotic (right) behaviours.

Similar results were obtained analyzing the time domain and frequency spectra of the state variables. The examples in Fig. 3 show the temporal evolution of all state variables, in the periodic and chaotic cases, for the same parameter values used before: $G$ = 100 and $a$ = 0.16, for period three multiplication, and $G$ = 100 and $a$ = 0.22, for chaos. In Fig. 4, power spectral densities are presented, for the same cases and parameter values.

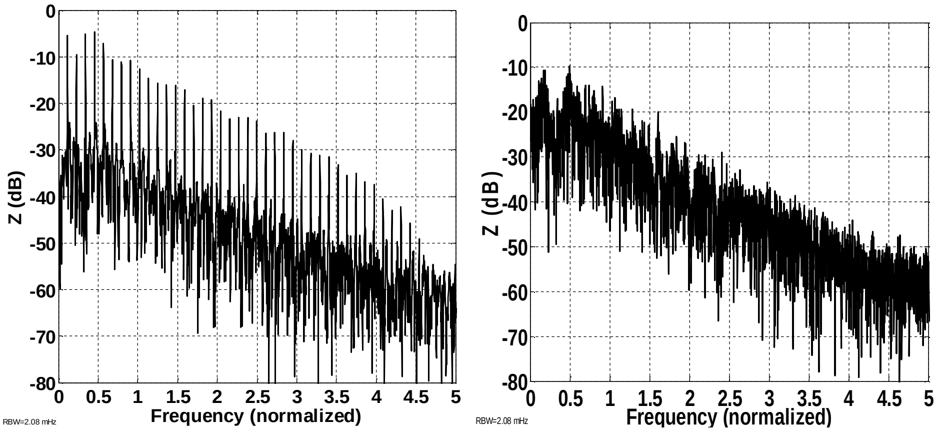

Fig. 4 – Power spectral densities of the state variable $z$ for periodic (left) and chaotic (right) behaviours.

## 3. The Synchronization Method

Our goal is to design a secure communication system with good encryption and masking properties, based on a setup as simple as possible. That is why we adopted the emitter partitioning method for chaos synchronization (Carrol *et al.*, 1991). The transmitted signal is the $z$ emitter state variable and the receiver is a simple observer, designed by copying the emitter first two state equations, with tilde state variable notation:

$$
(E:)\begin{cases} \mathrm{d}x/\mathrm{d}t = -ax + \omega y - z, \\ \mathrm{d}y/\mathrm{d}t = -\omega x + z, \\ \mathrm{d}z/\mathrm{d}t = -x - y - \omega z + \mathrm{sat}(x), \end{cases} \qquad (6)
$$

$$
(R:)\begin{cases} \mathrm{d}\tilde{x}/\mathrm{d}t = -a\tilde{x} + \omega\tilde{y} - z, \\ \mathrm{d}\tilde{y}/\mathrm{d}t = -\omega\tilde{x} + z. \end{cases}
$$

The obtained receiver is a linear system, with the state transition matrix:

$$
\mathbf{A} = \begin{bmatrix} -a & \omega \\ -\omega & 0 \end{bmatrix}. \qquad (7)
$$

The eigenvalues of the matrix **A** are:

$$\begin{cases} \lambda_1 = -\dfrac{a}{2} + j\dfrac{\sqrt{4\omega^2 - a^2}}{2}, \\ \lambda_2 = -\dfrac{a}{2} - j\dfrac{\sqrt{4\omega^2 - a^2}}{2}. \end{cases} \tag{8}$$

For all positive values of $a$, the receiver system is globally asymptotically stable, thus satisfying a necessary condition of synchronization.

In order to rigorously verify the global synchronization of the receiver with the emitter, we use the error dynamics method, denoting:

$$\begin{cases} \varepsilon_x = x - \tilde{x}, \\ \varepsilon_y = y - \tilde{y}. \end{cases} \tag{9}$$

Subtracting the receiver state equations from the corresponding emitter ones, in equation (4), we obtain the state equations of the error system:

$$\begin{cases} \mathrm{d}\varepsilon_x / \mathrm{d}t = -a\varepsilon_x + \omega\varepsilon_y, \\ \mathrm{d}\varepsilon_y / \mathrm{d}t = -\omega\varepsilon_x. \end{cases} \tag{10}$$

The error system is also linear and has the same state transition matrix as the receiver, (7). This leads to the conclusion that the error system is globally asymptotically stable, thus confirming synchronization of the receiver with the emitter.

To use the synchronizing communication channel, obtained by the previous analysis, in practical transmission, a modulation procedure must be developed. The most suitable alternative, for the emitter partition we previously performed, is to add the modulating signal to the third equation of the emitter:

$$\left(E_m :\right) \begin{cases} \mathrm{d}x/\mathrm{d}t = -ax + \omega y - z, \\ \mathrm{d}y/\mathrm{d}t = -\omega x + z, \\ \mathrm{d}z/\mathrm{d}t = -x - y - \omega z + \mathrm{sat}(x) + \omega m(t), \end{cases} \tag{11}$$

and append to the receiver a third equation, similar to the one in the emitter system, which performs the task of demodulation:

$$\left(R_{\tilde{m}} :\right) \begin{cases} \mathrm{d}\tilde{x}/\mathrm{d}t = -a\tilde{x} + \omega\tilde{y} - z, \\ \mathrm{d}\tilde{y}/\mathrm{d}t = -\omega\tilde{x} + z, \\ \mathrm{d}\tilde{z}/\mathrm{d}t = -\tilde{x} - \tilde{y} - \omega\tilde{z} + \mathrm{sat}(\tilde{x}), \\ \tilde{m}(t) = \varepsilon_z = z - \tilde{z}. \end{cases} \tag{12}$$

The output equation of the receiver system, (12), estimates the modulating signal, using the third state variable error, $\varepsilon_z$. The differential equation of the demodulated signal may be obtained by subtracting the third equation of the receiver, in (12) from its corresponding one for the emitter, in (11):

$$\frac{\mathrm{d}\tilde{m}}{\mathrm{d}t} = -\varepsilon_x + \left[\mathrm{sat}(x) - \mathrm{sat}(\tilde{x})\right] - \varepsilon_y - \omega\tilde{m} + \omega m(t). \tag{13}$$

After the synchronization transient has faded out, and the errors, $\varepsilon_x$ and $\varepsilon_y$, have become smaller than $1/G$, the differential equation of the demodulated signal becomes linear:

$$\frac{\mathrm{d}\tilde{m}}{\mathrm{d}t} = (G-1)\varepsilon_x - \varepsilon_y - \omega\tilde{m} + \omega m(t). \tag{14}$$

Finally, for small values of the error signals, $\varepsilon_x$ and $\varepsilon_y$, the differential equation of the demodulated signal may be approximated by neglecting the terms in $\varepsilon_x$ and $\varepsilon_y$:

$$\frac{\mathrm{d}\tilde{m}}{\mathrm{d}t} \approx -\omega\tilde{m} + \omega m(t). \tag{15}$$

For all positive values of $\omega$, the dynamics of the demodulated signal is a stable one, but the input-output relation of the modulation-demodulation system is frequency dependent, described by the transfer function:

$$H_D(s) = \frac{\tilde{M}(s)}{M(s)} = \frac{\omega}{s+\omega}. \tag{16}$$

If the $\omega$ coefficient is too small, the system passband may be inadequate for high speed data transmission, limiting the maximum effective frequency in the transmitted signal to $0.1\omega$, if both amplitude and phase distortions are to be reduced to an acceptable level. To compensate for this limitation, a linear equalizer may be included in the communication system:

$$H_E(s) = \frac{s+\omega}{1/K\,s+\omega}. \tag{17}$$

where $K$ is the factor by which we intend to increase the passband of the overall transmission system. Thus, the resulting communication system can be described by the global transfer function:

$$H(s) = H_D(s)H_E(s) = \frac{\omega}{s+\omega}\cdot\frac{s+\omega}{1/K\,s+\omega} = \frac{K\omega}{s+K\omega}. \tag{18}$$

As highlighted by the result in equation (18), the overall transmission system has a passband $K$ times larger than the initial one, leading to better speed performance, with minimum complexity increase.

## 4. Simulation Results

In order to verify the correctness of the synchronization setup, we performed several simulations for the system parameters ensuring chaotic behavior of the emitter, by applying sinusoidal modulating signals, with frequencies smaller than the communication system bandwidth:

$$B_v = K\omega. \tag{19}$$

The simulation results, as in the example shown in Fig. 5, confirm the asymptotic trend of the receiver state variables towards the values of the corresponding state variables of the emitter, leading to state errors decreasing to zero. Similarly, the error between the modulating signal and the demodulating one is also decreasing to zero, after a synchronization transient time of the order of magnitude of the system time constant:

$$\tau = 2/a\,. \tag{20}$$

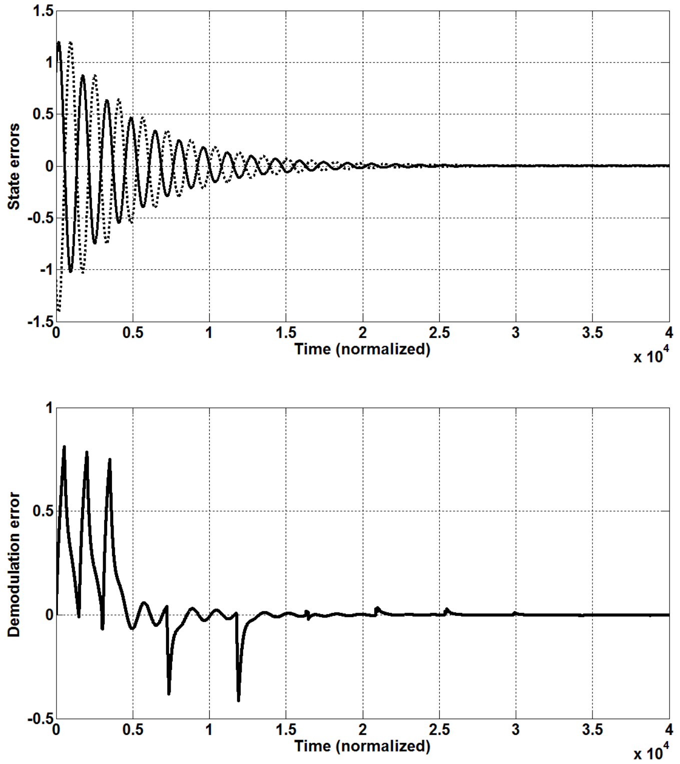

Fig. 5 – Synchronization error for the system state variables (up) and modulating – demodulated signals (down).

The efficiency of the linear feed-forward equalizer was verified by simulating data transmission over the chaotic channel. The modulating signal was chosen to be a periodic rectangular one, with amplitude approximately ten times smaller than the largest values of the state variables and frequency a decade over the cutoff value of the chaotic channel. In Fig. 6 we show an example of such simulation results, highlighting the amplitude distortion of the modulating signal due to the low-pass characteristic of the chaotic channel and the large amplitude of the demodulation error. These results lead to the conclusion that high speed data transmission is ineffective without proper equalization. Fig. 7 depicts the improvement obtained by using a linear feed-forward equalizer, with a factor of $K$ = 1,000 bandwidth increase. Not only the

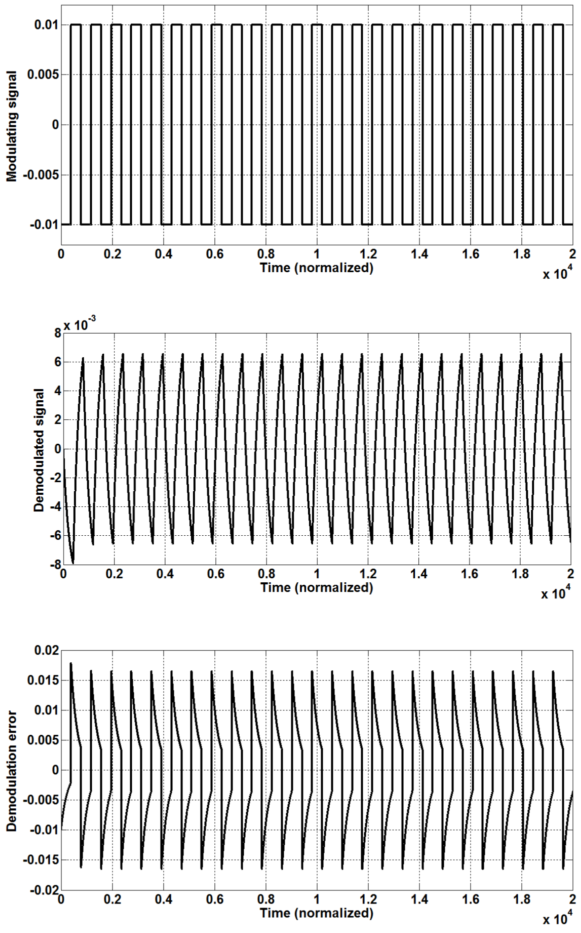

Fig. 6 – Demodulation results without feed forward equalizer: modulating signal (up), demodulated signal (middle) and demodulation error (down)

amplitude of the demodulation error is reduced by one order of magnitude, but also the time extent of the error pulses is greatly improved. As a consequence, the demodulated signal presented in Fig. 7 is mostly undistorted.

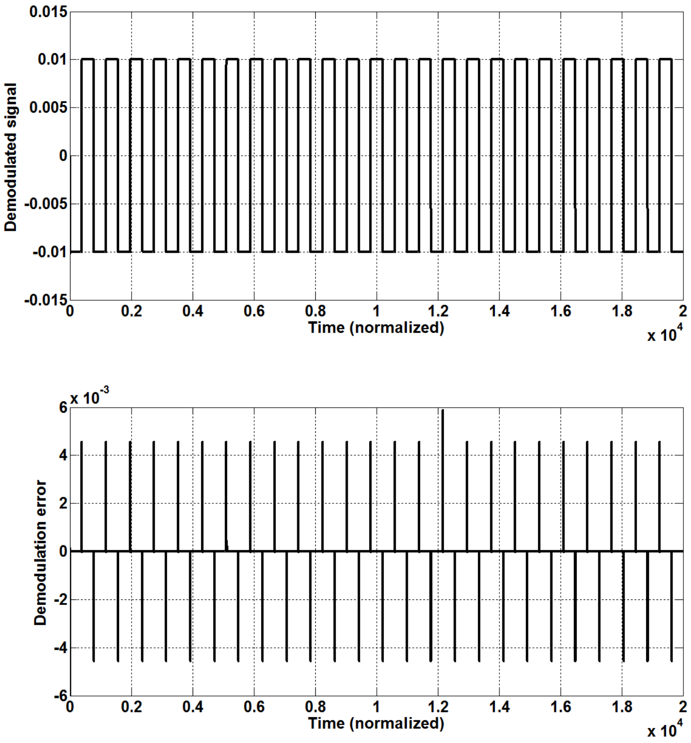

Fig.7 – Demodulation results with feed forward equalizer: demodulated signal (up) and demodulation error (down).

An important aspect to be analyzed is the system sensitivity to channel noise. Several simulations were made with band-limited, zero average, Gaussian white noise, for different values of the noise power. The example presented in Fig. 8, for a noise power of $10^{-13}$ W, shows that channel perturbation affects the amplitude of the data signal, but has little effect on the rectangular modulating signal fronts. This allows data recovery using a high speed comparator, thus making transmission over noisy channels possible.

In order to verify the transmission security based on the masking property of the chaotic modulation, the fact that the modulating signal is not visually identifiable in the transmitted signal waveform is not enough. Several simulations were made using spectral analysis of the modulated chaotic signal. The simulation results showed that, in order to hide well enough the modulating signal in the chaotic one, the amplitude of the modulating signal has to be at least one order of magnitude smaller than the transmitted signal.

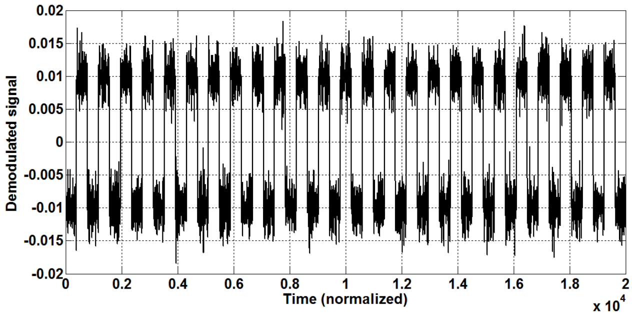

Fig. 8 – Demodulated signal affected by noise.

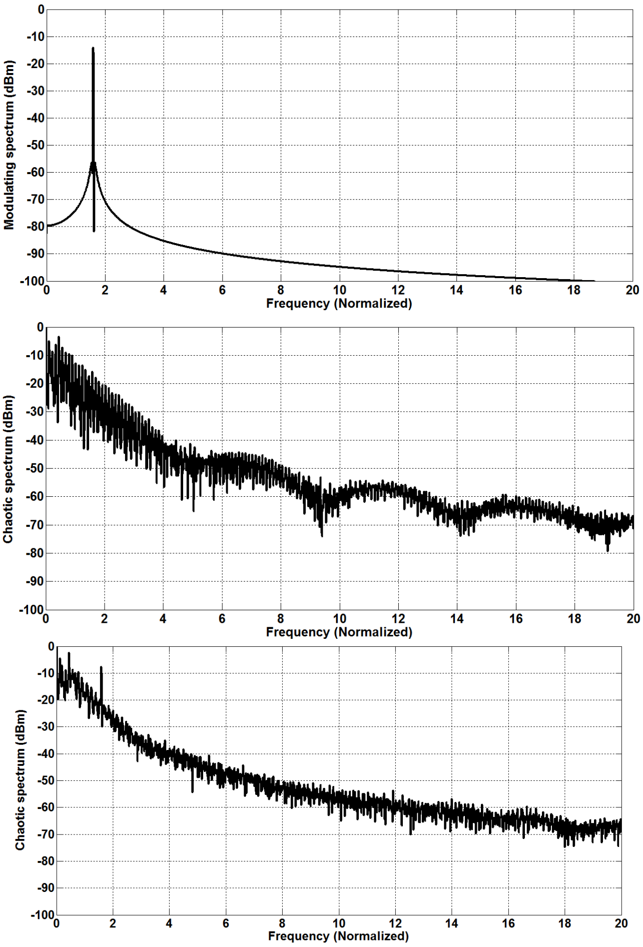

Fig. 9 – The PSD of the modulating signal (up) and of the chaotic signal, for modulating amplitude 0.01 (middle) and 0.1 (down).

For example, in Fig. 9, we show the spectra of the sinusoidal modulating signal and the chaotic one, highlighting that for comparable amplitudes the sine spectral line is visible in the power spectrum of the transmitted one, whereas for reduced modulating sine amplitude, the clear message is perfectly hidden.

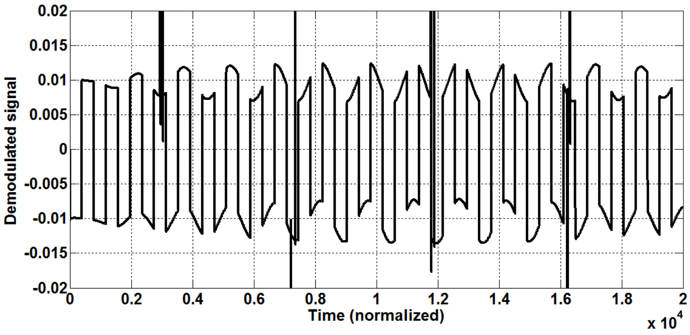

Fig. 10 – Demodulated signal affected by parameter mismatch.

Another security aspect is related to the communication system sensitivity to the parameter mismatch between the receiver and the emitter circuits. A low sensitivity will allow an unauthorized receiver to demodulate the transmitted message, if the structure of the emitter is unveiled. On the other hand, an extremely high sensitivity might create difficulties to the authorized receiver in recovering the modulating signal. Simulations performed on our system showed good sensitivity properties as depicted in Fig. 10.

## 5. Conclusions

We propose an analog secure communication system based on non-linear synchronization and direct modulation. Using the emitter system partitioning method of synchronization and error dynamics demodulation method, we demonstrated, in a general enough case, that a linear dynamic relation exists between the modulating signal applied at the emitter in the communication channel and its demodulated counterpart at the receiver end. For compensation, a feed-forward channel equalization technique is used to ensure that the modulating signals can have large enough bandwidth, leading to the possibility of high speed digital communication. The presented case studies highlight the feasibility of the general method in both analog and digital cases.

## REFERENCES

Carrol T.L., Pecorra L.M., *Synchronizing Chaotic Circuits*. IEEE Transactions on Circuits and Systems, **38**, *4*, 453-456 (1991).

Chua L.O., Gui-Nian Lin, *Canonical Realization of Chua's Circuit Family*. IEEE Trans. on Circ. a. Syst., **37**, *7*, 885-902 (1990), doi: 10.1109/31.55064.

Grigoraş V., Tătaru V., Grigoraş C., *Chaos Modulation Communication Channel: a Case Study*. Proc.of the Internat. Symp. on Sign. Circ. a. Syst., ISSCS2009, July 9-10, 2009, Iaşi, Romania, 489-492.

Grigoraş V., Grigoraş C., *Chaos Parameter Modulation Equalization*. Proc of the Internat. Conf. Commun., Bucharest, Romania, June 10–12, 2010, 33-36, doi: 10.1109/ICCOMM.2010.5509089.

Grigoraş V., Grigoraş C., *Dynamic and Statistic Analysis of a Simple Chaotic Generator*. Proc. of the IEEE Internat. Symp. on Sign., Circ. a. Syst., ISSCS2015, July 9-10, 2015, Iaşi, Romania, 122-125, doi: 10.1109/ ISSCS.2015.7204024.

Elwakil A.S., Kennedy M.P., *Construction of Classes of Circuit-Independent Chaotic Oscillators Using Passive-Only Nonlinear Devices*. IEEE Trans. on Circ. a. Syst., I: Fundamental Theory and Applications, **48**, *3*, 289-307 (2001).

Li C., Sprott J.C., Thio W., Zhu H., *A Unique Signum Switch for Chaos and Hyperchaos*. 7th Internat. Conf. on Phys. A. Control (PhysCon 2015), Istambul, Turkey, August 19-22, 2015.

## SISTEM DE COMUNICAŢII SECURIZAT BAZAT PE SINCRONIZARE HAOTICĂ ANALOGICĂ

(Rezumat)

Se prezintă proiectarea unui sistem de transmisiuni de date securizat bazat pe sincronizarea haotică şi modulaţia directă. Sistemul de comunicaţii propus este bazat pe un emiţător analogic simplu vizând posibilitatea implementării ieftine. Se prezintă sistemul haotic emiţător cu modificările adaptate scopului sincronizării şi modulaţiei şi se analizează comportarea sa dinamică neliniară. Sunt analizate de asemenea configuraţia generală a sistemului de transmisiuni de date, condiţiile de sincronizare şi demodulare corecte precum şi compensarea erorilor. În final sunt sugerate posibilităţile de aplicare în comunicaţiile analogice şi digitale.