SOME APPROACHES AND RESULTS ON COMMUNICATION SECURITY

Ion Tutănescu
E-mail: tutanescu@upit.ro
Department of Electronics and Computers, University of Pitesti, Romania

ABSTRACT

In this paper we present some of our applications on chaotic carrier systems, results and considerations on this field. One of our applications presented in the paper is the implementation of a Chua's circuit-based chaotic carrier communication system using operational amplifiers. Its operation is based on modulation of a chaotic oscillator signal by the informational signal. Next in the paper we present some of the methods that can be used in order to additionally increase the communication security. These methods combine the classic encryption with the synchronisation of chaotic systems, aiming to enhance the security level. Another presented application dwells on a digital chaotic carrier communication system that uses a digital filter with finite impulse response (FIR), in conjunction with its inverse filter, to implement an encrypter and a decrypter, respectively. Such a system is adaptive, meaning that the receiver adapts to the transmitter operation through a Least Mean Square (LMS) algorithm.

I. INTRODUCTION

A growing attention has been given in the last period of time to chaos-based transmission methods for using in the field of secure communications [3][5][8]. Basically, these methods consist in the information's representation as noise-like waves. The theory that based this new research field is the chaotic dynamic systems' theory which deals with the change of a system status in time. The solutions of a chaotic dynamic system can have variations in time for certain values of parameters and for other parameters' values the solutions have a deterministic (regular) behaviour. These variations seem randomly and the behaviour is named chaotic. Therefore, the noise-like waves are the solutions of some dynamic systems that in certain conditions have a chaotic behaviour. In the time domain the signals generated by dynamic systems are randomly, their auto-correlation function having a peak in origin and decreasing very fast in the rest; in the frequency domain the signals have a wide spectrum. These chaotic systems generate signals which have much of the random processes' properties, but have a determinist structure that makes these systems to be reproducible. There are analogic chaotic systems and digital chaotic systems. Several chaos-based communication systems (also known as chaotic carrier communication systems) were conceived, studied, simulated, implemented and tested in order to evaluate their performances [1][3][4][11][12]. A series of problems were highlighted: the chaotic carrier systems' mathematical modelling, analysis of adopted models, generation of the chaotic signals, modulation and demodulation methods, synchronisation methods between transmitter and receiver.

II. CHAOTIC CARRIER COMMUNICATIONS SYSTEMS

In order to produce chaotic signals, there are different generators (see Figure 1) using:

a) natural noise sources (resistors, diodes),

b) shift registers (digital filters),

c) nonlinear dynamic systems with chaotic behaviour.

There are continuous time generators and discrete time generators. As a continuous time chaotic generator the Chua circuit is well-known (see Figure 2). Other such generators are: RLC circuit with nonlinear resistance, nonlinear RC circuit, LC/RC oscillators with chaotic behaviour.

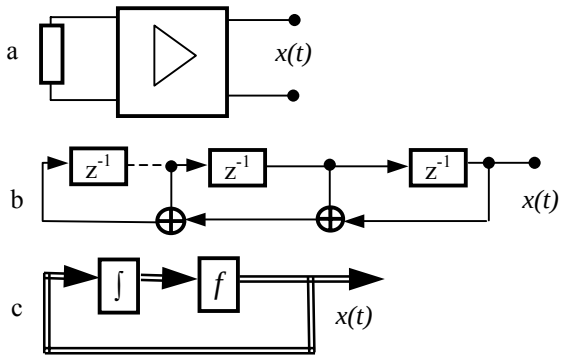

Figure 1. Continuous time chaotic generators: a - using natural sources, b - with shift registers, c - using nonlinear dynamic systems.

b

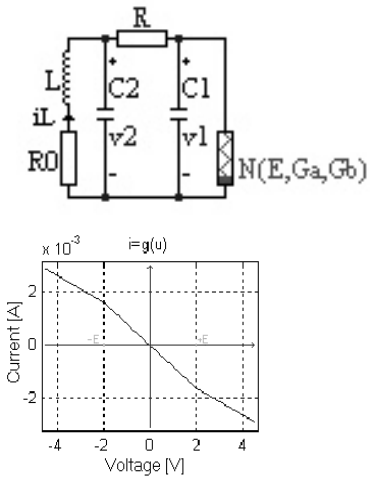

Figure 2. a - Electrical scheme of Chua circuit, b -Current-voltage diagram of Chua circuit.

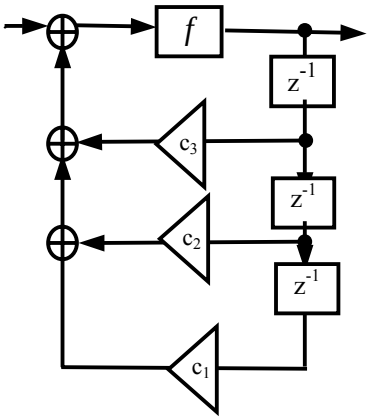

Figure 3. Chaotic generator realised with a digital filter.

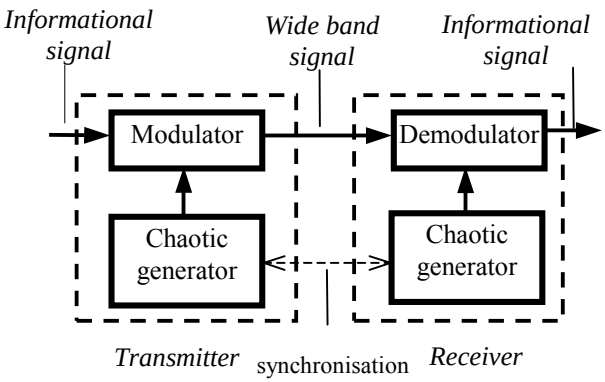

Figure 4. The general structure of a chaotic carrier communications system.

As discrete time chaotic generators are generally used digital filters [1][3][4]. An example of generator realised with digital filters is shown in Figure 3.

For realising protected communications it is necessary to modulate the chaotic signal with the informational signal. The general structure of a chaotic carrier communication system is presented in Figure 4.

For a proper operation it is necessary to have absolutely identical chaotic generators in transmitter and in receiver.

The most used modulation methods are: chaotic masking, chaotic parametrical modulation, chaotic direct modulation, Chaos Shift Keying (CSK) modulation, Differential Chaos Shift Keying (DCSK) modulation, etc. [5][6][11].

The chaotic dynamic systems have an unpredictable behaviour on long term. A chaotic dynamic system has a specific compact state space, named attractor.

The evolutions of two identical chaotic dynamic systems (with the same attractor), but starting in the state space from two close points, will diverge after a certain time, although the evolutions "stay" inside the same attractor. For this is necessary to synchronise the two systems.

The most used methods of synchronisation are: "master - slave" synchronisation, error's feedback synchronisation, observer's method, inverse system's method, method using synchronisation pulses, dead-beat synchronisation, etc. [11].

III. IMPLEMENTATION OF A CHAOTIC CARRIER COMMUNICATION SYSTEM

We implemented a chaotic carrier communication system based on the modulation of a chaotic oscillator's parameter by the informational signal. There was used a Chua chaotic circuit. Transmitter's electrical scheme is presented in Figure 5.

The transmitter's mathematical description is given by the following differential equation system:

$$\begin{cases} \dfrac{dx}{d\tau} = \alpha\left[y - (1+\gamma)x - \phi(x) + \gamma\lambda\right]; \\ \dfrac{dy}{d\tau} = x - y + z; \\ \dfrac{dz}{d\tau} = -\beta\, y; \end{cases} \qquad (1)$$

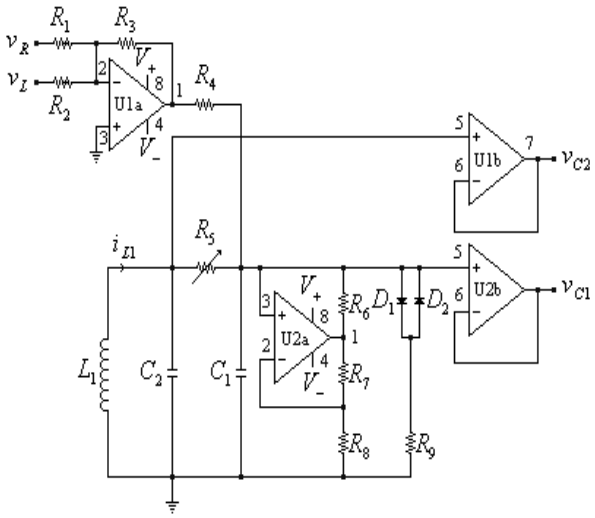

Figure 5. The transmitter's electrical scheme.

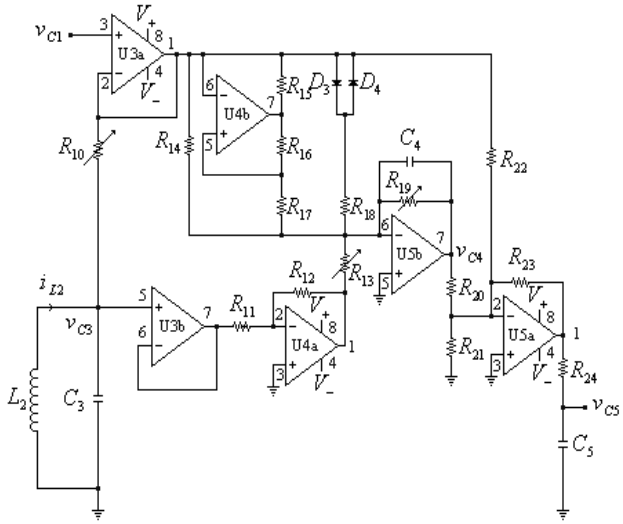

Figure 6. The receiver's electrical scheme.

where:

$$\phi(x) = ax + \left(\frac{b-a}{2}\right)\left(|x+1| - |x-1|\right) \tag{2}$$

and

$$\tau = \frac{t}{R_5 C_2}. \tag{3}$$

The state variables are:

$$x = \frac{v_{C1}}{V_{on}};\ y = \frac{v_{C2}}{V_{on}};\ z = \frac{R_5 i_{L1}}{V_{on}}, \tag{4}$$

where V_{on} = 0,7 V represents the diode's breakout voltage. The system's parameters are defined as bellow:

$$\begin{cases} \alpha = \dfrac{C_2}{C_1}; \\ \beta = \dfrac{R_5^2 C_2}{L_1}; \\ \gamma = \dfrac{R_5}{R_4}; \\ a = \dfrac{R_5}{R_2} - \dfrac{R_5 R_7}{R_6 R_8}; \\ b = -\dfrac{R_5 R_7}{R_6 R_8}. \end{cases} \tag{5}$$

The modulation parameter λ is given by:

$$\lambda = \frac{R_3}{V_{on}}\left(\frac{v_R}{R_1} + \frac{v_L}{R_2}\right). \tag{6}$$

The receiver is presented in Figure 6:

The receiver is characterised by the following differential equations system:

$$\begin{cases} \dfrac{dy_r}{d\tau} = x - y_r + z_r; \\ \dfrac{dz_r}{d\tau} = -\beta y_r; \\ \dfrac{dw_0}{d\tau} = \alpha\left[y_r - (1+\gamma)x - \phi(x)\right] + kx - kw_0; \\ \dfrac{d\lambda_f}{d\tau} = q_f\left[\dfrac{w_0 - x}{\gamma} - \lambda_f\right]. \end{cases} \tag{7}$$

Because of the specific way for realising the modulation, we have $w_1 = 1/\gamma$ when $\tau \to +\infty$. The receiver's state values are:

$$y_r = \frac{v_{C3}}{V_{on}};\ z_r = \frac{R_{10} i_{L2}}{V_{on}};\ w_0 = \frac{v_{C4}}{V_{on}};\ \lambda_f = \frac{v_{C5}}{\gamma V_{on}}.$$

The two constants of the receiver's filter are:

$$\begin{cases} k = \alpha; \\ q_f = \dfrac{R_5 C_2}{R_{24} C_5}. \end{cases} \tag{8}$$

We excited the transmitter at the input with sinusoidal, rectangular and FSK (Frequency Shift Keying) signals.

In this paper we present the results obtained in laboratory for FSK input informational signals (see Figure 7).

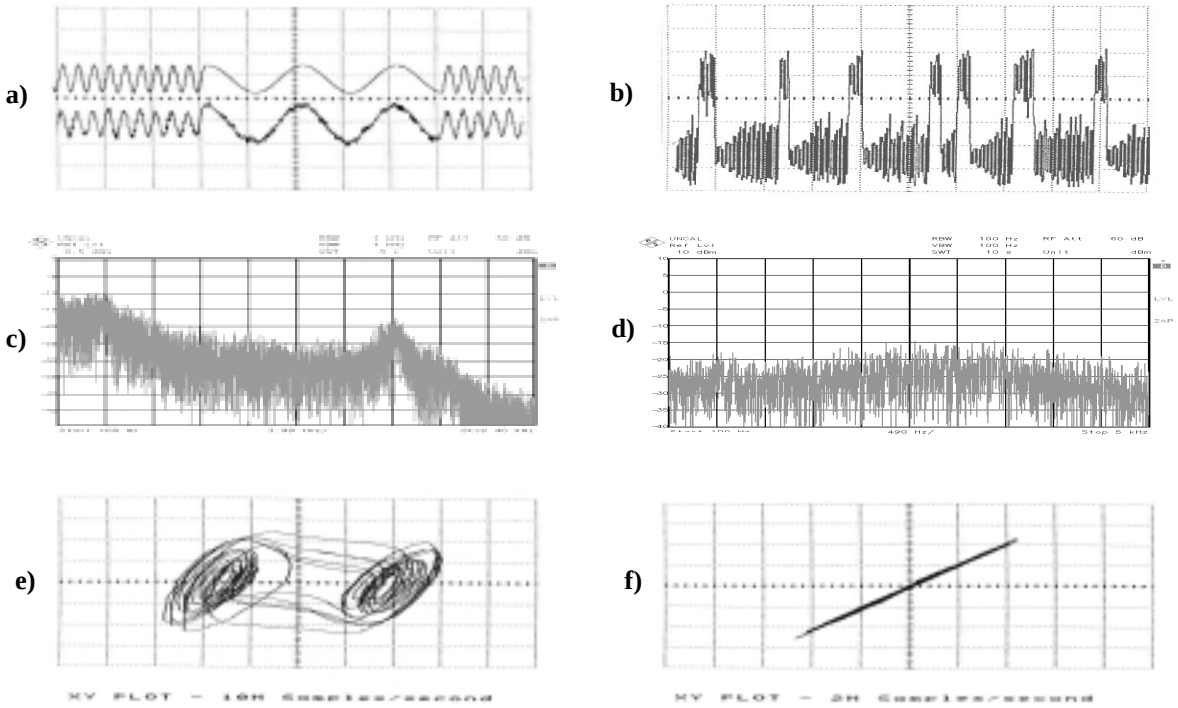

Figure 7. Some of the laboratory experimental results: a) FSK input informational signal (up) and output recovered signal (down), b) Masked signal transmitted in communication channel, c) Frequency spectrum of masked signal (100 Hz - 40 KHz), d) Zoom of the frequency spectrum in the region 100 Hz - 5 KHz, e) The attractor generated by the transmitter, f) Synchronisation between transmitter and receiver when the input signal is applied.

The implemented Chua's circuit-based communication system has a good practical behaviour in laboratory conditions.

The receiver recovers very well the input informational signal (Figure 7a). What is very important is that the masked signal (Figure 7b) has roughly the same form for the three input signals (sinusoidal, rectangular and FSK).

The level of masked signal's spectral components are higher in 100 Hz - 5 KHz frequency range with 15 - 25 dBm than in the rest of the spectrum (Figure 7c) and is quite constant in that range (Figure 7d); this fact determine us to take 100 Hz - 5 KHz range as masked signal frequency band.

The obtained attractor (Figure 7e) has two lobes, typical for Chua's circuit. The system synchronisation is put in evidence in Figure 7f, without having applied at input a signal, and is kept when there are applied input signals not greater than 0.8 volts peak-to-peak.

This requirement for applying small input signals could be in contradiction with the practical need to use greater signals so as the communication channel's noise will not affect signal recovery in receiver. Using an error's detection and correction code, the system performance in noise conditions could be improved. The system was not experimented yet in real conditions for the communication channel: attenuation, noise, distortions, frequency band limitation, etc.

IV. INCREASE OF SECURITY

Next we present in this paper some of the methods that can be used in order to additionally increase the communication security. The more complex is the transmitted signal, the higher is the security of the communication system.

These proposed methods combine the classic encryption with the synchronisation of chaotic systems, aiming to enhance the security level. In order to hide the contents of a message using chaotic signals different techniques have been developed. Basically, for increasing the interception resistance of the chaotic carrier communications, three classes of methods are used:

a) use of digital filters having a chaotic behaviour together with nonlinear mapping functions,

b) use of digital filters having a chaotic behaviour together with binary shift registers, shift cipher and auto-key ciphers,

c) use of chaotic systems involving two chaotic signals: first for the chaotic encrypter and decrypter synchronisation and the other for informational signal encryption using a classical encryption algorithm (by example, shift ciphers).

The intruder needs to reconstruct the key signal which is different from the transmitted signal. It seems very difficult to create reconstruction methods in order to obtain the key signal. Such methods have not been reported so far. The general block diagram of a Chua's circuit-based cryptosystem is presented in Figure 8, where $v_R(t)$ is the transmitted signal, $v_2(t)$ is the key signal and $p(t)$ is the plain (message) signal.

The state equations of this cryptosystem are described bellow.

- For the encrypter:

$$\begin{cases} \dfrac{dv_1}{dt} = \dfrac{1}{C_1}\left[\dfrac{1}{R}(v_2 - v_1) - f(v_R)\right]; \\ \dfrac{dv_2}{dt} = \dfrac{1}{C_2}\left[\dfrac{1}{R}(v_1 - v_2) + i_L\right]; \\ \dfrac{di_L}{dt} = \dfrac{1}{L}(-v_2). \end{cases} \quad (9)$$

where $f(\ )$ is the nonlinear characteristics of Chua's diode from Chua's circuit, given by

$$f(v_1) = G_b v_R + \frac{1}{2}(G_a - G_b)\left[|v_1 + E| - |v_1 - E|\right]. \quad (10)$$

E is the breakpoint voltage of Chua's diode. The voltage v_R is given by:

$$v_R = v_1 - e(p(t)), \quad (11)$$

where $e(p(t))$ represents the encrypted signal.

- For the decrypter:

$$\begin{cases} \dfrac{dv_1}{dt} = \dfrac{1}{C_1}\left[\dfrac{1}{R}(\tilde{v}_2 - \tilde{v}_1) - f(v_R)\right]; \\ \dfrac{dv_2}{dt} = \dfrac{1}{C_2}\left[\dfrac{1}{R}(\tilde{v}_1 - \tilde{v}_2) + i_L\right]; \\ \dfrac{di_L}{dt} = \dfrac{1}{L}(-\tilde{v}_2). \end{cases} \quad (12)$$

$$\tilde{e}(p(t)) = \tilde{v}_1 - v_R, \quad (13)$$

where $\tilde{e}(p(t))$ is the encrypted signal, recovered by receiver.

For the plain signal encryption a n-shift cipher is used. It is defined by the relation:

$$e(p(t)) = \underbrace{f_1(\ldots f_1(f_1(p(t), \underbrace{v_2(t)), v_2(t)) \ldots , v_2(t))}_{n}}_{n} = y(t),$$

where $f_1(*, *)$ is a nonlinear function described by:

$$f_1(x,k) = \begin{cases} (x+k) + 2h, & for\ -2h \le (x+k) \le -h; \\ (x+k), & for\ -h < (x+k) < -h; \\ (x+k) - 2h, & for\ h \le (x+k) \le 2h. \end{cases} \quad (14)$$

and h is chosen such that $p(t)$ and $v_2(t)$ lie within $(-h, h)$.

The decryption rule is similar with the encryption:

$$p(t) = d(y(t)) = e(y(t)) = f_1(\ldots f_1(f_1(y(t), -\tilde{v}_2(t)), -\tilde{v}_2(t)) \ldots , -\tilde{v}_2(t)) = y(t), \quad (15)$$

where $\tilde{v}_2(t)$ is recovered by the receiver and should approximate $v_2(t)$.

The key signal $v_2(t)$ is used n times to encrypt the plain signal. Because the encrypted signal is a function of $v_2(t)$ and $p(t)$ and since the encrypted signal is used to drive the Chua's circuit, it hides both the dynamical and the statistical characteristics of $v_2(t)$ and $p(t)$.A different approach uses two chaotic signals [7][8]: one of them is used for the chaotic encrypter and decrypter synchronisation, the other signal is used for informational signal encryption using a encryption scheme, by example with shift ciphers. The general block diagram of the chaos-based cryptosystem is represented in Figure 9.

The encrypter consists of a chaotic system and an encryption function $e(t)$. The cryptographic key $k(t)$ is one of the state variables of the chaotic system.

The transmitted signal $s(t)$ is another state variable of the chaotic system. It is sent through a public channel to the decrypter and used to synchronise the decrypter.

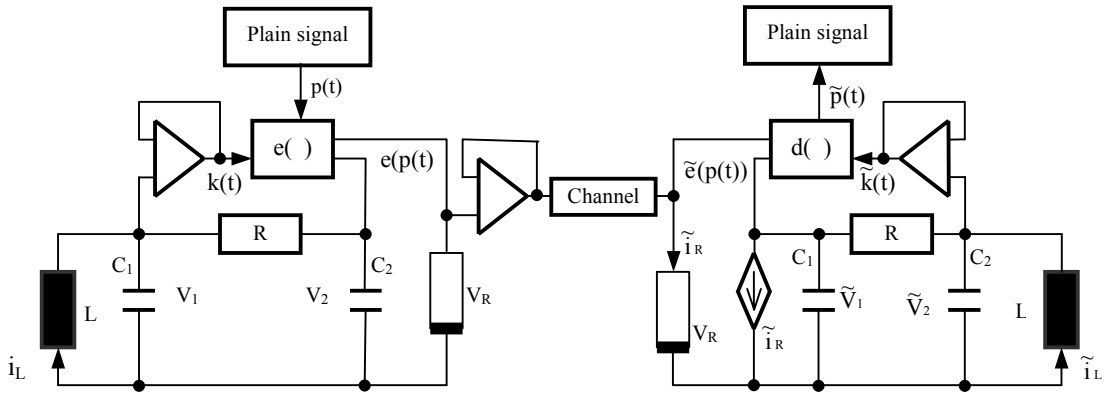

Figure 8. The general block diagram of a Chua's circuit-based cryptosystem.

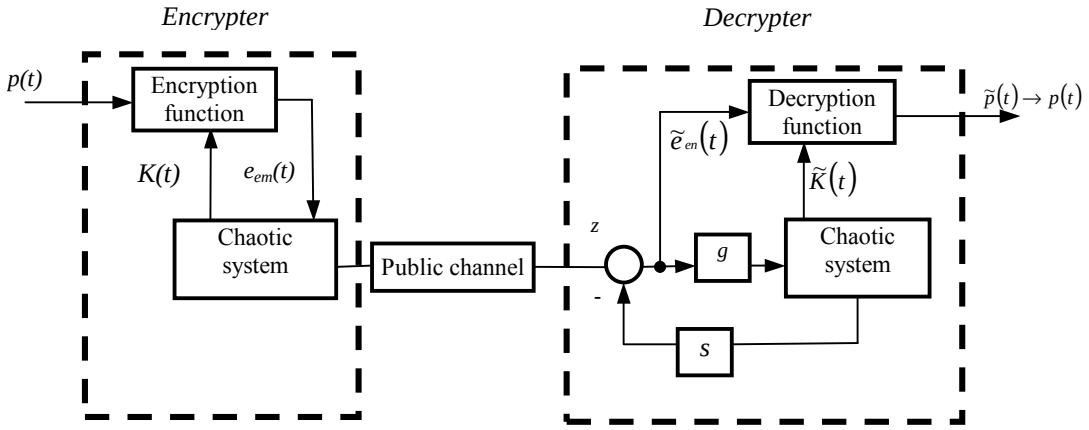

Figure 9. The block diagram of the chaos-based cryptosystem.

The decrypter consists of a chaotic system and a decryption function *d*( ). It should be noted that both the encrypted signal *y(t)* and the key signal *k(t)* are not sent to the decrypter. It is different from traditional discrete cryptosystems where both the encrypted signal and the key should be transmitted to the decrypter.

The communication channel's noise *n(t)* is added to *s(t)*, so the decrypter receives the sum signal *z(t)= s(t) + n(t).*

Only when the decrypter and the encrypter are synchronised, the decrypter can find the encrypted signal and the key signal. Then, the decryption function *d*( ) is used to decrypt the encrypted signal.

V. DESIGN AND SIMULATION OF A DIGITAL CHAOTIC CARRIER COMMUNICATION SYSTEM

The analogic chaos-based communication systems suffer from some drawbacks in practice. Since two matched analogic chaotic circuits are required at remote locations, in practice there can be serious problems with system performance, unless a method of calibration is devised.

It was demonstrated that digital filters can be used in chaotic systems [1][2]. In some papers [3][4][5] are proposed digital filters-based chaotic systems.The digital filter-based encrypter must have quasy-chaotic properties (*QC-properties*) in order to have a quasy-chaotic behaviour and therefore to be of value in secure communications applications [3].

Such an encrypter that respects QC-properties can be used for the communications encryption. The encrypter and the decrypter obey the following defining equations:

- Encrypter:

$x(n)=h_1(n) * u(n) + h_2(n)*F(x(n), x(n - 1), \dots , x(n - M));$

$e(n) = d(n)* x(n);$

- Decrypter:

$x(n) = \bar{d}(n) * e(n);$

$x(n)= \bar{h}_1(n) *u(n)+ \bar{h}_2(n) *F(x(n), x(n - 1),\dots,x(n - M)).$

where:

- *u(n)* - is the input sequence (plain signal),
- *x(n)* - is an internal signal,
- *e(n)* - is the encrypted signal to be transmitted to the receiver,
- *y(n)* - is the output sequence (decrypted signal),
- $h_1(n)$, $h_2(n)$, ... - IIR (Infinite Impulse Response) or FIR (Finite Impulse Response),
- *F*(.) - is a general nonlinear map suited to hardware implementation,
- + and * - are the addition and convolution operators.

The encrypter must respect the QC-properties and the decrypter must realise the inverse function of the encrypter.

We propose a digital filter-based chaotic cryptosystem that makes possible a good adaptation of the receiver to transmitter.

The proposed scheme is shown in Figure 10. The encrypter is a feedback system consisting of a nonlinear function *f(x)* given by:

$$f(x) = x - 2 * \left[\frac{x+1}{2} \right], \qquad (16)$$

(where [.] represents the integer part of the number located between square parenthesis) and a FIR digital filter in the feedback loop:

$$H_{BF}(z) = \sum_{i=1}^{N} h_i z^{-i}. \qquad (17)$$

For $x \in [-1,+1]$ the encrypter has the following transfer function:

$$H_T(z) = \frac{1}{1 - H_{FB}(z)} = \frac{1}{1 - \sum_{i=1}^{N} h_i z^{-i}}. \qquad (18)$$

The encrypter will have a chaotic behaviour if its transfer function has poles located outside of the unit circle.

The decrypter is the inverse system of encrypter. It consists of a FIR digital filter having the transfer function

$$H_R(z) = 1 - H_{FB}(z) = 1 - \sum_{i=1}^{N} \bar{h}_i z^{-i}. \quad (19)$$

and a nonlinear function, identical with the function $f(.)$ from encrypter.

The two nonlinear systems (encrypter and decrypter) are better described by the discrete time equations.

- Encrypter:

$$y[k] = f\left(m[k] + \sum_{i=1}^{N} h_i y[k-i]\right) = \\ = m[k] + \sum_{i=1}^{N} h_i y[k-i] - 2 * s[k], \quad (20)$$

where

$$s[k] = \left[\frac{1 + m[k] + \sum_{i=1}^{N} h_i y[k-i]}{2}\right].$$

- Decrypter:

$$\bar{m}[k] = f\left(m[k] + \sum_{i=1}^{N} \bar{h}_i y[k-i]\right) = \\ = y[k] - \sum_{i=1}^{N} \bar{h}_i y[k-i] - 2 * \bar{s}[k], \quad (21)$$

where

$$\bar{s}[k] = \left[\frac{1 + y[k] - \sum_{i=1}^{N} \bar{h}_i y[k-i]}{2}\right].$$

If $m[k]$ modulator signal amplitude is small and the coefficients of the digital filters used in encrypter and decrypter are identical, the synchronisation is achieved in $N+1$ clock periods. The output signal is the copy of plain (input) signal.

The adaptive algorithm uses a gradient-based method. If we note with $E(\bar{h})$ the measuring error that should be minimised, we could write:

$$\bar{h}[k+1] = \bar{h}[k] - \mu * \frac{\partial E\left(\bar{h}\right)}{\partial \bar{h}}, \quad (22)$$

(5)

where $\bar{h}$ is a N-dimensional vector of decrypter filter coefficients and μ is the algorithm adaptation step.

If the error function is considered to be equal with the square of instantaneous signal value given by decrypter, $E\left(\bar{h}\right) = \bar{m}^2[k]$, the classical adaptive algorithm Least Mean Square (LMS) is obtained.

With this algorithm are obtained good results. So,

$$\bar{h}[k+1] = \bar{h}[k] + 2 * \mu * \bar{m}[k] * Y[k], \quad (23)$$

where (6)

$$Y[k] = [y[k-1], y[k-2], ..., y[k-N]]^T.$$

Simulations were realised with third order FIR digital filters, using a number n = 8192 points, a sampling frequency f_s = 98 KHz and a informational signal's binary flow D_b = 2400 bits/second. Also we used the following data for the initial conditions of the transmitter Y_{0T} = [y_{0T}(-2), y_{0T}(-1), y_{0T}(0)] and of the receiver, Y_{0R} = [y_{0R}(-2), y_{0R}(-1), y_{0R}(0)].

The filter coefficients were h_{0T} = [h_{1T}, h_{2T}, h_{3T}] and h_{0R} = [h_{1R}, h_{2R}, h_{3R}]:

$$\begin{cases} Y_{0T} = [-.1 \; -.15 \; -.3]^T \\ Y_{0R} = [-1.2 \; -1 \; -.08]^T \\ h_{0T} = [1.5 \; -1.3 \; 2] \\ h_{0R} = [2.2 \; -2 \; 3] \end{cases}$$

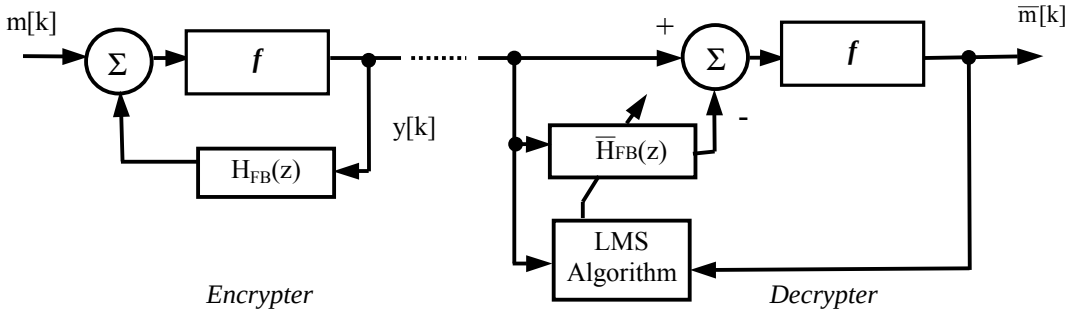

Figure 10. The block diagram of the adaptive digital filter-based chaotic cryptosystem.

The simulation results are shown in Figure 11.

The decrypter's digital filter coefficients go to those of the encrypter's digital filter after approximately 25 ms and then the decrypter is synchronised with the encrypter. Once the synchronisation is realised, the decrypter keeps synchronisation with the encrypter.

The chaotic signal sent in the communication channel has very fast variations and its shape is complex. So, informational signal is very well hidden in transmitted chaotic signal.

After the synchronisation is achieved, the recovered signal has approximately the same shape as the input signal.

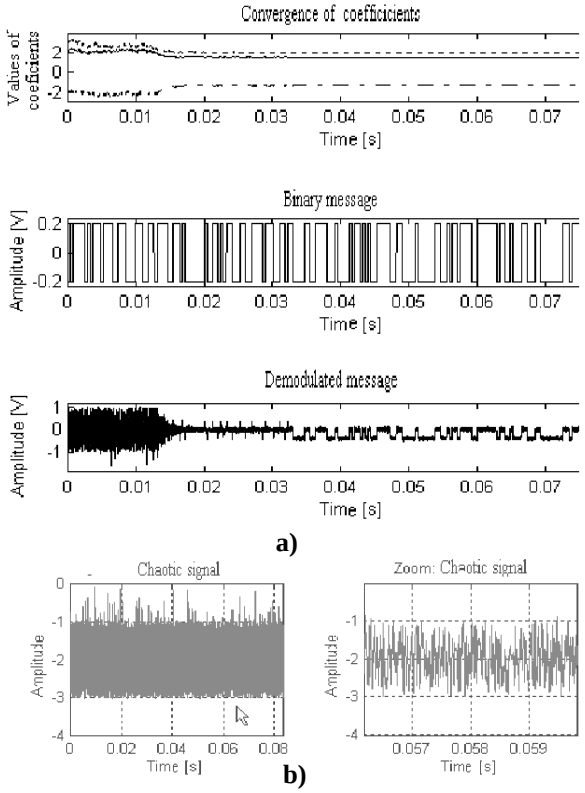

Figure 11. Some of the computer simulations' results: a) Convergence of digital filters' coefficients (up), input informational signal (middle) and output recovered informational signal (down), b) Masked chaotic signal transmitted in the communication channel.

CONCLUSION

Because of properties they have, the chaotic carrier communication systems are a viable alternative to the existing communication systems. The chaotic carrier communication systems provide a good level of security because of chaotic signals used for transmission. Using the chaotic wide frequency band signals, these systems are noise-resistant.

The research is to be continued for improving the performances, especially for increasing of modulation (transmission) speed, in real conditions of operation.

REFERENCES

[1] D.R. Frey, "Chaotic Digital Encoding: An Approach to Secure Communication", IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing, Vol. 40, No. 10, Octob. 1993, pp. 660-666;

[2] D.R. Frey, "On Adaptive Chaotic Encoding", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 45, No. 11, November 1998, pp. 1200-1204;

[3] L.O. Chua, T. Lin, "Chaos in digital filters", IEEE Transactions on Circuits and Systems, Vol. 35, June 1998, pp. 648-658;

[4] L.O. Chua, T. Lin, "Chaos and fractals from third-order digital filters", Int. J. Circuit Theory Appl., Vol. 18, May-June 1990, pp. 241-255;

[5] M. Götz, K. Kelber, W. Schwarz, "Discrete-Time Chaotic Encryption Systems - Parts I, II and III, IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications, Vol. 44, No. 10, October 1997, pp. 963-970/ Vol. 45, No. 2, February 1998/ Vol. 45, No. 9, September 1998, pp. 983-988;

[6] U. Feldman, M. Hasler, W. Schwarz, "Communication by Chaotic Signals: Inverse System Approach", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Appl., Vol. 42, No. 2, February 1995;

[7] I. Tutănescu, C. Irimia, A. Şerbănescu, "Design and simulation of a chaotic based cryptosystem", International Conference "Communications 2000" Proceedings, Bucharest, 7-9 Dec. 2000, pp. 381-385;

[8] T. Yang, C.W. Wu, L.O. Chua, "Cryptography based on Chaotic Systems", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 44, No. 5, May 1997, pp. 469-472;

[9] G. Grassi, S. Mascolo, "A System Theory Approach for Designing Crypto-systems Based on Hyperchaos", IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications, Vol. 46, No. 9, September 1999, pp. 1135-1138;

[10] A. Leuciuc, V. Grigoraş, "Simulation Results on Discrete-Time Filter Adaptive Chaos Synchronisation", ECCTD'97, Budapest, Sept. 1997;

[11] A. Şerbănescu, "Sisteme de transmisiuni integrate, Vol.1 - Comunicaţii de bandă largă folosind sisteme dinamice haotice", Editura Academiei Tehnice Militare, Bucureşti, 2000;

[12] A. Şerbănescu, I. Tutănescu, E. Sofron, D. Scheianu, C. Irimia, "Applications of Chaotic Dynamic Systems", International Conference ECIT 2002, Iaşi, Romania.