



DISCRETE IMPLEMENTATION OF CHAOTIC ENCRYPTION SYSTEM

Carmen GRIGORAȘ^{1,2}, Victor GRIGORAȘ³

¹“Gr.T. Popa” University of Medicine and Pharmacy of Iași, 700115, Romania

²Institute of Computer Science of the Romanian Academy, Iași, 700481, Romania

³“Gheorghe Asachi” Technical University of Iași, 700506, Romania

Corresponding author: Victor GRIGORAȘ, E-mail: grigoras@etti.tuiasi.ro

Abstract. Chaotic systems have a number of applications, digital encryption being one of the most attracting ones. The present paper aims at taking an analogue nonlinear system prototype to develop the desired chaotically encrypted communication line in a discrete-time structure. The proposed discrete nonlinear system is designed based on chaotic synchronization approach. The designed architecture is intended for secure communication applications and the obtained performance is estimated both dynamically and statistically.

Key words: chaos encryption, nonlinear dynamics, digital implementation, discrete systems.

1. INTRODUCTION

Nonlinear systems can perform a number of dynamical behaviors such as constant, periodic, quasi-periodic and chaotic. Chaotic systems have several applications especially in noise and random binary codes generation [1–3], chaotic modulation [4, 5], spread-spectrum clock signal generation [6] and complex natural systems modeling [7]. From the engineering point of view, one of the most attracting applications is chaotic encryption [8–10], due to its communications usefulness and better sensitivity control.

The present contribution intends to present the design of a discrete-time chaotic encryption system based on a previously developed hysteretic analogue emitter prototype. The presented research is motivated by the desire to apply the analogue system taken as starting point in encryption applications and the aim of digitally implement the discrete-time synchronizing communication system. It is also important to highlight the interest of researchers in studying hysteresis nonlinear systems [11–13], although previous results aim at much simpler systems and do not approach chaotic synchronization as an application. The proposed discrete emitter is designed applying the Euler discretization method to the previously introduced [14] fourth order analog nonlinear circuit, using a Schmitt trigger hysteresis non-linearity. Compared to previously reported systems, the prototype emitter yields more complex dynamics, with both double scroll and two single scroll strange attractors, suggesting better encryption performance. The obtained discrete-time emitter preserves the dynamic complexity of the analog prototype as shown in the bifurcation diagrams and chaotic attractor projections. The presented statistical properties of the proposed emitter, including histograms and frequency spectra, also highlight the complexity of the emitted signal. The synchronization short-time transient and state error decreasing to zero sustain the proposed chaotic encryption application of the digital communication system. In order to use this analogue nonlinear prototype for secure communication, a synchronizing receiver is designed based on the emitter system partitioning method. The implementation of the proposed design is programmable digital, with advantages studied in previous references [15, 16].

The paper is structured in four sections. The next one presents the design of the proposed discrete-time encryption emitter and receiver nonlinear systems. The third section shows the results of the encryption line simulations, including parameter determination and synchronization errors. The concluding remarks highlight the performance of the designed system.

2. THE DISCRETE-TIME SYSTEM DESIGN

In order to design the discrete emitter-receiver pair for secure data transmission, an analog model is used as starting point. The analogue chaotic emitter (E_a), first introduced in [13], is a modulated generator with hysteresis nonlinearity, described by the fourth order state equations:

$$(E_a :) \begin{cases} \frac{dx_E}{dt} = -a \cdot x_E + \omega_0 \cdot y_E - z_E \\ \frac{dy_E}{dt} = -\omega_0 \cdot x_E + z_E \\ \frac{dz_E}{dt} = -x_E - y_E - \omega_0 \cdot z_E + \text{sat}(v_E) + m(t) \\ \frac{dv_E}{dt} = b \cdot x_E - c \cdot v_E + d \cdot \text{sat}(v_E). \end{cases} \quad (1)$$

In the differential equations (1), the modulating signal, $m(t)$, is the useful signal chaotically encrypted to be securely transmitted and the algebraic function $\text{sat}(\cdot)$ is:

$$\text{sat}(x) = \begin{cases} 1 & x > 1 \\ x & -1 < x < 1 \\ -1 & x < -1. \end{cases} \quad (2)$$

In the referenced paper [13], the b , c , and d coefficients are calculated based on physical values related to analog implementation. Due to the digital version intended here, they will remain generic values, independent to physical measurements.

The analogue receiver, (R_a), designed by using the emitter partitioning method, is characterized by the state equations:

$$(R_a :) \begin{cases} \frac{dx_R}{dt} = -a \cdot x_R + \omega_0 \cdot y_R - z_E \\ \frac{dy_R}{dt} = -\omega_0 \cdot x_R + z_E \\ \frac{dz_R}{dt} = -x_R - y_R - \omega_0 \cdot z_R + \text{sat}(v_R) \\ \frac{dv_R}{dt} = b \cdot x_R - c \cdot v_R + d \cdot \text{sat}(v_R). \end{cases} \quad (3)$$

Notably, the transmitted signal from the chaotic emitter to the synchronizing receiver, is the third emitter state variable $z_E(t)$. The demodulator used at the receiver end of the channel, recovers the useful signal $\tilde{m}(t)$, as a difference between emitter and receiver z state variables:

$$\tilde{m}(t) = z_E(t) - z_R(t). \quad (4)$$

In order to preserve the order of the emitter and receiver systems, we choose to use the Euler discretization method to deduce the state equations of the discrete-time communication system:

$$\frac{dx}{dt} \approx \frac{1}{T} (x(t_{k+1}) - x(t_k)). \quad (5)$$

In equation (5), x is a generic state variable and T denotes the clock period of the discrete-time emitter and receiver systems, equal to the sampling period of the discrete-time signals:

$$x[k] = x(t_k); \quad x[k+1] = x(t_{k+1}); \quad T = t_{k+1} - t_k, \quad k \in \mathbb{Z} \dots \quad (6)$$

By applying the approximation in (5) to the analogue emitter state equations (1), we obtain the state equations of the discrete-time emitter, $(E_d:)$, as detailed in equation (7)

$$(E_d:) \begin{cases} x_E[k+1] = x_E[k] + T(-a \cdot x_E[k] + \omega_0 \cdot y_E[k] - z_E[k]) \\ y_E[k+1] = y_E[k] + T(-\omega_0 \cdot x_E[k] + z_E[k]) \\ z_E[k+1] = z_E[k] + T(-x_E[k] - y_E[k] - \omega_0 \cdot z_E[k] + \text{sat}(v_E[k]) + m[k]) \\ v_E[k+1] = v_E[k] + T(b \cdot x_E[k] - c \cdot v_E[k] + d \cdot \text{sat}(v_E[k])) \end{cases} \quad (7)$$

Correspondingly, the state equations of the discrete-time receiver, $(R_d:)$, are obtained by applying the approximation (5) to the analogue receiver $(R_a:)$ state equations (3):

$$(R_d:) \begin{cases} x_R[k+1] = x_R[k] + T(-a \cdot x_R[k] + \omega_0 \cdot y_R[k] - z_E[k]) \\ y_R[k+1] = y_R[k] + T(-\omega_0 \cdot x_R[k] + z_E[k]) \\ z_R[k+1] = z_R[k] + T(-x_R[k] - y_R[k] - \omega_0 \cdot z_R[k] + \text{sat}(v_R[k])) \\ v_R[k+1] = v_R[k] + T(b \cdot x_R[k] - c \cdot v_R[k] + d \cdot \text{sat}(v_R[k])) \end{cases} \quad (8)$$

The synchronization error for the discrete emitter-receiver case is given by the error vector:

$$\boldsymbol{\varepsilon}[k] = \begin{bmatrix} \varepsilon_x[k] \\ \varepsilon_y[k] \\ \varepsilon_z[k] \\ \varepsilon_v[k] \end{bmatrix} = \begin{bmatrix} x_E[k] - x_R[k] \\ y_E[k] - y_R[k] \\ z_E[k] - z_R[k] \\ v_E[k] - v_R[k] \end{bmatrix}. \quad (9)$$

Combining the discrete-time state equations of the emitter (7) and receiver (8) with the error vector definition (9), the error dynamics $(\varepsilon:)$ equations are obtained:

$$(\varepsilon:) \begin{cases} \varepsilon_x[k+1] = \varepsilon_x[k] + T(-a \cdot \varepsilon_x[k] + \omega_0 \cdot \varepsilon_y[k]) \\ \varepsilon_y[k+1] = \varepsilon_y[k] + T(-\omega_0 \cdot \varepsilon_x[k]) \\ \varepsilon_z[k+1] = (1 - \omega_0 \cdot T) \varepsilon_z[k] + T(-\varepsilon_x[k] - \varepsilon_y[k] + \text{sat}(v_E[k]) - \text{sat}(v_R[k]) + m[k]) \\ \varepsilon_v[k+1] = \varepsilon_v[k] + T(b \cdot \varepsilon_x[k] - c \cdot \varepsilon_v[k] + d \cdot \text{sat}(v_E[k]) - d \cdot \text{sat}(v_R[k])) \end{cases} \quad (10)$$

The linearized version of the error dynamics equations is obtained by considering the small signal approximation of the nonlinear function $\text{sat}(\cdot)$, (11), to be applied to the equations (10):

$$\text{sat}(v_E[k]) - \text{sat}(v_R[k]) \approx v_E[k] - v_R[k] = \varepsilon_v[k]. \quad (11)$$

Taking this approximation into account, we obtain the linearized, non-autonomous error dynamics equations:

$$(\varepsilon_{lin}:) \begin{cases} \varepsilon_x[k+1] = (1 - aT) \varepsilon_x[k] + \omega_0 T \cdot \varepsilon_y[k] \\ \varepsilon_y[k+1] = -\omega_0 T \cdot \varepsilon_x[k] + \varepsilon_y[k] \\ \varepsilon_z[k+1] = (1 - \omega_0 \cdot T) \varepsilon_z[k] + T(-\varepsilon_x[k] - \varepsilon_y[k] + \varepsilon_v[k] + m[k]) \\ \varepsilon_v[k+1] = -bT \cdot \varepsilon_x[k] + (1 + dT - cT) \varepsilon_v[k] \end{cases} \quad (12)$$

The resulting state-transition matrix, \mathbf{A}_ε , for the linearized error dynamics system (12), results as presented in equation (13):

$$\mathbf{A}_\varepsilon = \begin{pmatrix} 1-aT & \omega_0 T & 0 & 0 \\ -\omega_0 T & 1 & 0 & 0 \\ -1 & -1 & 1-\omega_0 T & 1 \\ -bT & 0 & 0 & 1+T(d-c) \end{pmatrix}. \quad (13)$$

This leads to the eigenvalues vector λ_ε :

$$\lambda_\varepsilon = \begin{bmatrix} 1 - \frac{aT}{2} + \frac{T}{2} \cdot \sqrt{a^2 - 4 \cdot \omega_0^2} \\ 1 - \frac{aT}{2} - \frac{T}{2} \cdot \sqrt{a^2 - 4 \cdot \omega_0^2} \\ 1 - \omega_0 T \\ 1 + T(d - c) \end{bmatrix}. \quad (14)$$

In most usual application cases, the damping coefficient, a , is small enough compared to the natural oscillating frequency, ω_0 , allowing the approximation:

$$0 < a \leq 2\omega_0 \Rightarrow a^2 - 4 \cdot \omega_0^2 < 0. \quad (15)$$

In such cases, the state transition matrix eigenvalues are:

$$\begin{aligned} \lambda_{x,y} &\cong 1 - \frac{aT}{2} \pm j \frac{T}{2} \sqrt{4\omega_0^2 - a^2} \in \mathbb{C} \\ \lambda_z &= 1 - \omega_0 \cdot T \in \mathbb{R} \\ \lambda_v &= 1 + T(d - c) \in \mathbb{R} \end{aligned} \quad (16)$$

The linear error dynamics system (12) is stable, with synchronization errors decreasing to zero if the modulus of the state transition matrix eigenvalues is under unit:

$$\begin{aligned} |\lambda_{x,y}| &= \sqrt{1 - aT + \omega_0^2 T^2} < 1 \\ |\lambda_z| < 1 &\Rightarrow 0 < \omega_0 < 2/T \\ |\lambda_v| < 1 &\Rightarrow -2/T < d - c < 0. \end{aligned} \quad (17)$$

The previous conditions ensure emitter-receiver systems synchronization. If these conditions are fulfilled, the nonlinear synchronization error vector (9) decreases to zero, as suggested by the three-dimensional projection example depicted in Fig. 1, for the system parameters: $\omega_0 = 1.1$, $a = 0.1$, $b = 10^5$, $c = 3.51$, $d = 0.11$ and $T = 0.01$.

$$w_0 = 1.1, \quad a = 0.1, \quad b = 10^5, \quad c = 3.51, \quad d = 0.11, \quad T = 0.01. \quad (18)$$

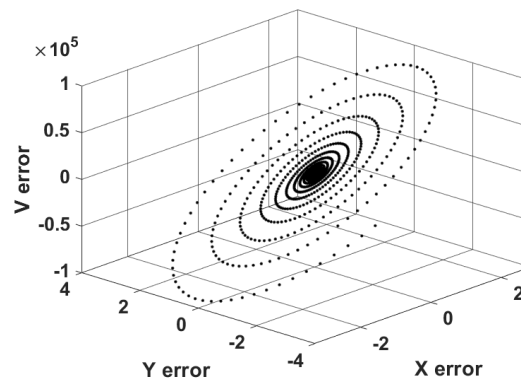


Fig. 1 – Three-dimensional projection on the x - y - v sub-space of the discrete synchronization error.

Although the error equations (10) are nonlinear, the decrease is dominated by the linear part and the depicted spiral is not visibly distorted. More important for communication applications, the demodulating process has small errors after a short synchronization transient. The example in Fig. 2, shows the correct demodulation after a transient of approximatively 3 200 samples, i.e. 32 seconds for $T = 0.01$.

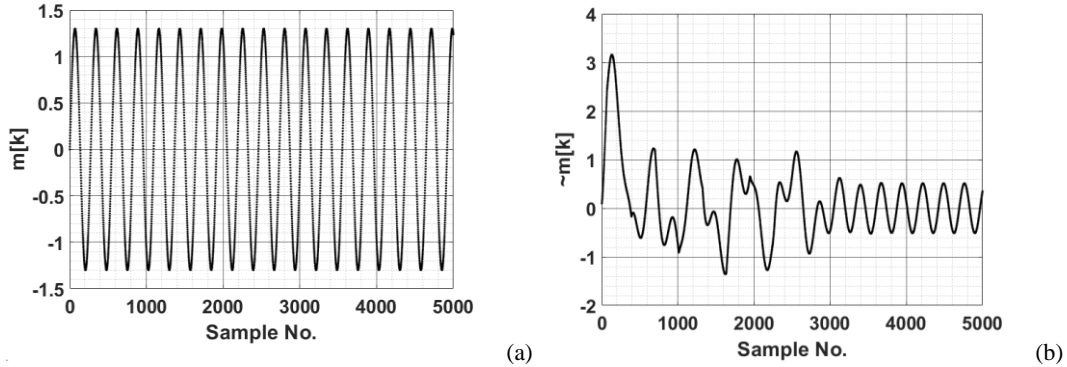


Fig. 2 – Modulating signal $m[k]$ (a) and demodulated signal $\sim m[k]$ (b).

3. DIGITAL IMPLEMENTATION

For the digital implementation, we chose a processor of the ARM Cortex M4 core with 32-bit architecture that allows high level language programming. The processor used in the tested implementation is STMicroelectronics STM32F334R8T6 and the generated signals were acquired with a Tektronix TDS2002B oscilloscope, digital results being saved and graphically represented. This processor has sufficient computing power to perform the calculations imposed by the nonlinear algebraic functions comprised in the difference state equations of the nonlinear system to be implemented. The D/A converters, included in the microcontroller structure, have 12 bits conversion capability, reasonable for interfacing the tested digital system with the analogue world. Due to the high enough number representation in the chosen processor, the number of bits in the conversion structure leads to the dominating differences between floating point simulation results and the corresponding digital measurements.

The algorithm used in the program implementation is suggested by the system state equations and leads to the following emitter-receiver pseudo code:

```
// emitter
initialize (emitter actual state vector);
while switch not pressed;
    convert A/D modulating signal  $m(t) \rightarrow m[k]$ ;
    compute state function (emitter actual state vector);
    store result in (next state vector);
    transfer (next state vector) > (actual state vector);
    convert D/A transmitted signal  $z[k] \rightarrow z(t)$ ;
end while;

// receiver
initialize (receiver actual state vector);
while switch not pressed;
    convert A/D received signal  $z(t) \rightarrow z[k]$ ;
    compute state function (receiver actual state vector);
    store result in (receiver next state vector);
    transfer (next state vector) > (actual state vector);
    convert D/A demodulated signal  $\sim m[k] \rightarrow \sim m(t)$ ;
end while;
```

The data structures needed for this simple algorithm is based upon two vectors with four floating point components, implemented for both emitter and receiver:

```
emitter actual state vector;
emitter next state vector;
receiver actual state vector;
receiver next state vector;
```

Added to the vector data structures, the scalar system parameters a , w , b , c , and d are also needed for correct program flow.

To develop the proposed nonlinear discrete design in a quantitative way, a parametric analysis can lead us to the equation coefficient values aiming the chaotic dynamics useful for encryption. By using bifurcation diagrams, we highlight the fact that the emitter behaves chaotically for a large range of values of the parameters, with small intervals of periodic behavior. Examples of such diagrams are presented in Fig. 3, for the c and d system coefficients. Similar results were obtained for the a and b parameters.

Using the equation coefficient sets in the value ranges suggested by the bifurcation diagrams, the emitter state variables highlight their chaotic evolution, as suggested in the example two-dimensional projections of the obtained attractor depicted in Fig. 4 for parameter choice (18).

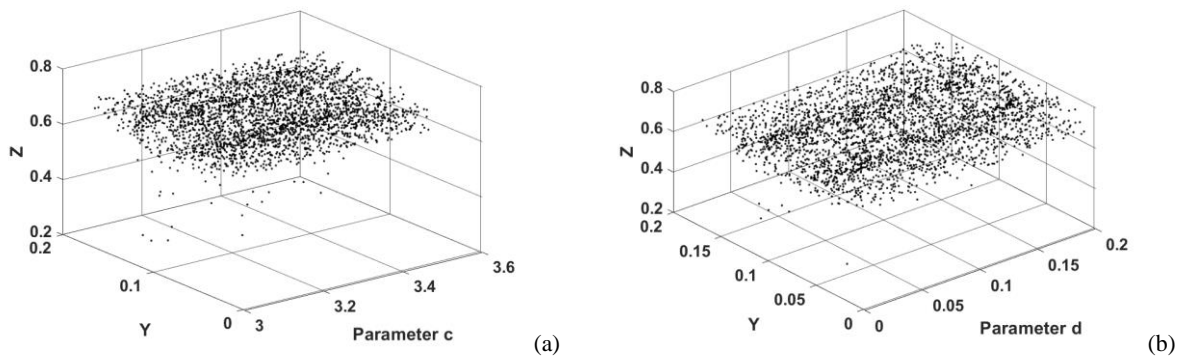


Fig. 3 – Bifurcation diagrams for the state variables $y[k]$ and $z[k]$ at the variation of parameters c (a) and d (b).

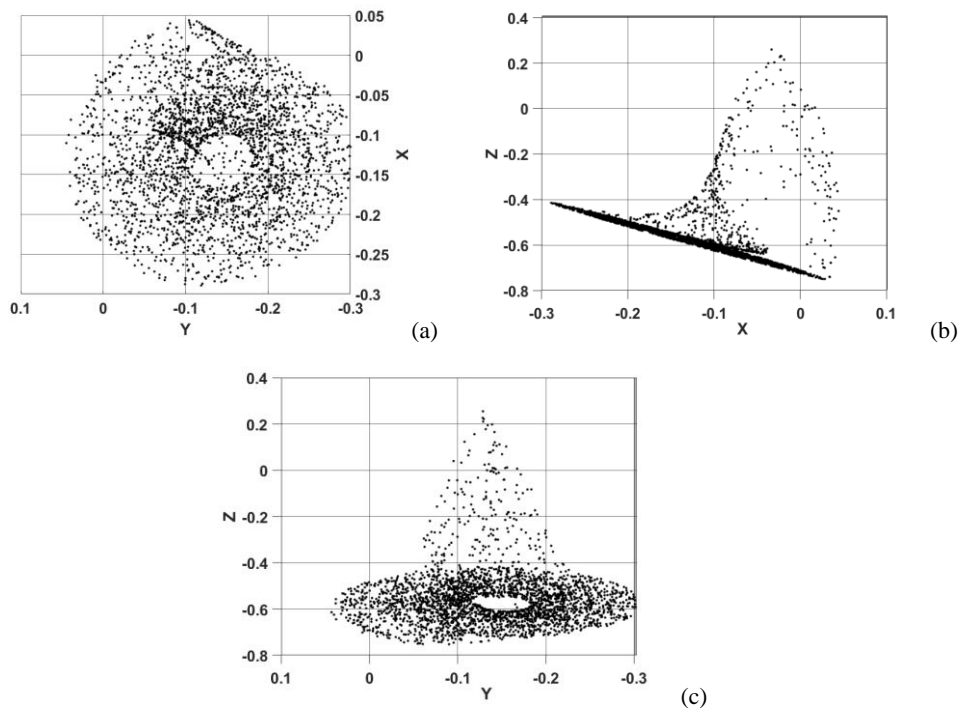


Fig. 4 – Two-dimensional projections of the chaotic attractor for the discrete-time system on planes x - y (a), x - z (b), and y - z (c).

From the statistical point of view, the emitter behavior was analyzed and examples of the obtained results are shown in Figs. 5, for histograms and Figs. 6, for frequency spectra, using the same parameter set of values (18) tested in the dynamic analysis too.

In the histograms depicted in Figs. 5, the large probability of extended ranges of values, mainly negative ones are obvious. The ranges may be approximated as $-0.25, \dots, 0$ for $x[k]$ and $y[k]$, $-0.8, \dots, 0$ for $v[k]$, finally $-0.7, \dots, -0.4$ for $z[k]$. Except for the last estimated state variable, $z[k]$, all other three exhibit two probability maxima, as a result of the chaotic attractor shape.

In the frequency domain, the power spectra estimations depicted in Fig. 6, exhibit a sufficiently large spectral extension, especially toward low frequencies, to justify uncorrelated state variables values, resulting from the chaotic emitter behavior.

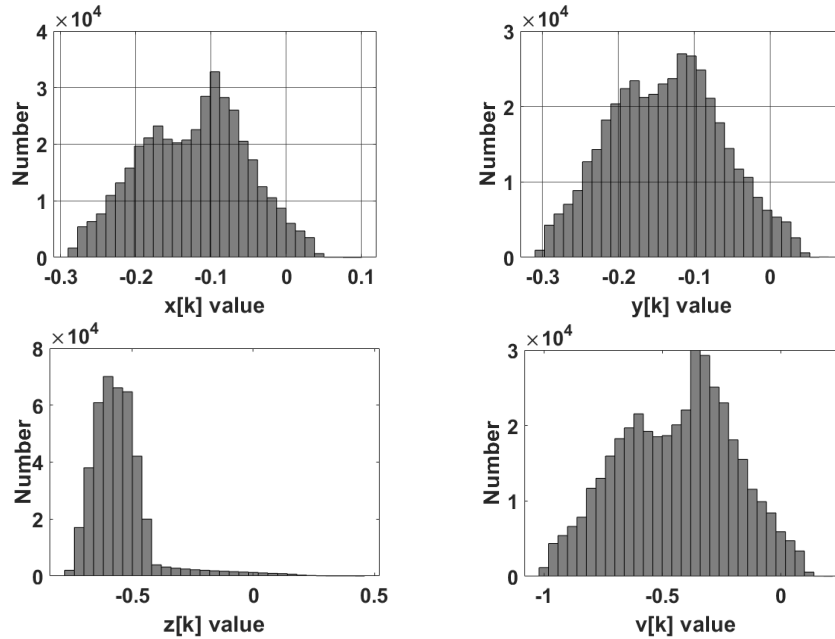


Fig. 5 – Digital emitter state variables histograms for all four state variables x , y , z , v .

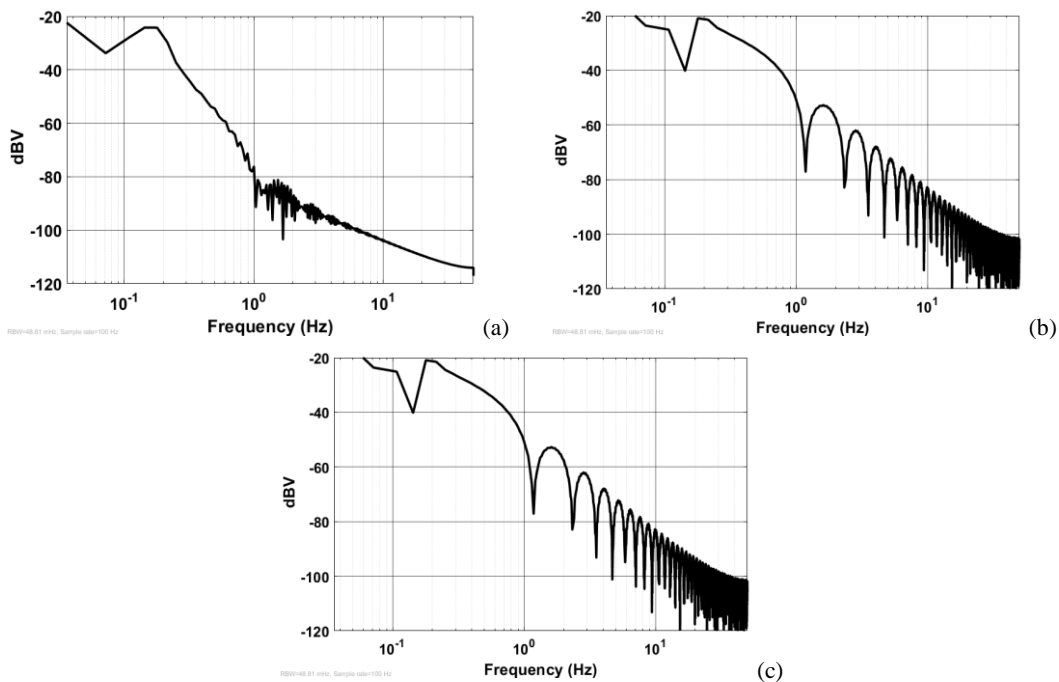


Fig. 6 – Emitter spectra for the discrete state variables $x[k]$ (a), $y[k]$ (b), and $z[k]$ (c).

4. CONCLUSION

The proposed discrete-time encrypted communication system is designed starting from a hysteretic analogue prototype for the chaotic emitter. The corresponding receiver is designed based on the synchronization method of the emitter partitioning system. From the analog emitter-receiver channel, the desired discrete version is deduced by applying the Euler sampling approximation, leading to a discrete communication system of the same order of complexity as the analog model. The obtained discrete-time state equations confirm the synchronization process, analyzed by the error dynamics method and showing short-time transient and state error decreasing to zero. The dynamic complexity of the discrete-time emitter is highlighted by bifurcation diagrams and strange attractor projections. The synchronization communication system performance is also sustained by statistical properties, such as histograms and frequency spectra.

The obtained discrete system leads to an algorithm allowing the desired programmable digital implementation on an ARM processor. The high order of the emitter generator and the relatively high number of encryption key parameters ensure a secure transmission of the useful modulating signal. Estimating the resulting digital encryption system performance is important for application purposes and it is performed both dynamically and statistically, highlighting its possible application in secured, low frequency biomedical and sound transmission.

REFERENCES

1. T. STOJANOVSKY, L. KOCAREV, *Chaos-based random number generators – Part I: Analysis*, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, **48**, 3, pp. 281–288, 2001.
2. T. ENDO, J. YOKOTA, *Generation of white noise by using chaos in practical phase locked loop integrated circuit module*, Proc. International Symposium on Circuits and Systems, pp. 201–204, 2007.
3. S. CALLEGARI, G. SETTI, *ADCs, chaos and TRNGs: a generalized view exploiting Markov chain lumpability properties*, Proc. International Symposium on Circuits and Systems, pp. 213–216, 2007.
4. V. GRIGORAS, V. TATARU, C. GRIGORAS, *Chaos modulation communication channel: a case study*, Proc. International Symposium on Signals, Circuits and Systems (ISSCS), 2009, pp. 489–492.
5. M. HASLER, T. SCHIMMING, *Chaos communication over noisy channels*, Int. J. of Bifurcation and Chaos, **10**, 4, pp. 719–736, 2000.
6. V. GRIGORAS, C. GRIGORAS, *Chaos based spread spectrum clock generator*, WSEAS – Transactions on Circuits and Systems, **4**, 8, pp. 1104–1111, 2005.
7. H.-N. TEODORESCU, V. COJOCARU, *Complex signal generators based on capacitors and on piezoelectric loads*, Chaos Theory: Modeling, Simulation and Applications, World Scientific Publishing Co., 2011, pp. 423–430.
8. S. CELIKOVSKY, V. LYNNYK, M. SEBEK, *Observer-based chaos synchronization in the generalized chaotic Lorenz systems and its application to secure encryption*, 45th IEEE Conference on Decision and Control, 2006, pp. 3783–3788.
9. A.S. ANDREATOS, C.K. VOLOS, *Secure text encryption based on hardware chaotic noise generator*, 2nd International Conference on Cryptography and its Applications in the Armed Forces, 2014.
10. V. GRIGORAS, C. GRIGORAS, *Time variant chaos encryption*, Chaos Theory: Modeling, Simulation and Applications, 2014, pp. 175–182.
11. C. LI, J.C. SPROTT, W. THIO, H. ZHU, *A unique signum switch for chaos and hyperchaos*, 7th International Conference on Physics and Control (PhysCon), 2015, pp. 19–22.
12. T. TSUBONE, T. SAITO, *On basic piecewise-constant systems*, Proc. International Symposium on Circuits and Systems (ISCAS 2000), **1**, Geneva, Switzerland, pp. 248–251, May 2000, DOI: 10.1109/ISCAS.2000.857074.
13. T. TSUBONE, K. HOSHINO, T. SAITO, *Bifurcation from a 3-D hysteresis piecewise-constant circuit*, Proc. of the International Symposium on Circuits and Systems (ISCAS 2001), **3**, Sydney, Australia, 2001, pp. 815–818.
14. C. GRIGORAS, V. GRIGORAS, *Complex dynamics in hysteretic nonlinear oscillator circuit*, Proceedings of the Romanian Academy – Series A Mathematics, Physics, Technical Sciences, Information Science, **18**, 4, 2017, pp. 370–377.
15. H.T. YANG, R.J. HUANG, T.I. CHANG, *A chaos-based fully digital 120 MHz pseudo random number generator*, Proc. IEEE Asia-Pacific Conference on Circuits and Systems, 2004, pp. 357–360.
16. H. NEJATI, A. BEIRAMI, W.H. ALI, *Discrete-time chaotic-map truly random number generators: design, implementation, and variability analysis of the zigzag map*, Analog Integr. Circ. Sig. Process, **73**, 1, 2012, pp. 363–374.

Received December 14, 2020