Implementation of Chaotic Systems for Secure Communications in Embedded DSP System

ROGER CHIU, JUAN H. GARCIA-LOPEZ, RIDER JAIMES –REATEGUI, EDGAR VILLAFAÑA-RAUDA, CARLOS E. CASTAÑEDA-HERNANDEZ, GUILLERMO HUERTA-CUELLAR AND DIDIER LOPEZ-MANCILLA
Departamento de Ciencias Exactas y Tecnología
Centro Universitario de los Lagos, Universidad de Guadalajara
Enrique DÍaz de León 1144, Lagos de Moreno, Jalisco. 47463
MEXICO
rchiuzar@gmail.com

Abstract: - In this work, we present results about the implementation of chaotic generators with DSPs, which were programmed in C language. The main idea is about the synthesis of chaotic generators using DSK 5510 Texas instrument development card. The Lorenz system, Rössler system and Chua's circuit were used for this purpose.

Key-Words: -Chaotic oscillators, DSP, Lorenz system, Rössler system, Chua's circuit.

1 Introduction

As Continuous chaos has, under the name of deterministic nonperiodic flow, been first described by E.N. Lorenz in model of turbulence [1]. Lorenz's equation consists of three coupled ordinary differential equations, which contain two nonlinear terms (of second order, xz and xy) [2]: $\dot{x} = 10(y - x), \dot{y} = x(28 - z) - y, \dot{z} = xy - (8/3)x$. Chaotic systems provide a rich mechanism for signal designing and generation, with potential applications in communications and signal processing. In 1976, Otto E. Rössler [2] constructed the following three-dimensional system of differential equations:
$\dot{x} = -(y + z), \dot{y} = x + ay, \dot{z} = b + xz - cz$,where a, b, and c are all constants[3]. Elementary electric circuit theory was introduced in the mid-1980s., Chua [3,4] modeled a circuit that was a simple oscillator exhibiting a variety of bifurcation and chaotic phenomena, in the simple case, Chua´s equations can be written in the following dimensionless form: $\dot{x} = \alpha(y - x - g(x)), \dot{y} = x - y + z, \dot{z} = -\beta y - \gamma z,$
$g(x) = cx + (1/2)(d - c)(|x+1| - |x-1|)$. Because chaotic signals are typically broadband, noise like, and difficult to predict, they can be used in various contexts for masking information-bearing waveforms. They can also be used as modulating waveforms in spread spectrum systems [5]. Since Pecora and Carroll reported their work on synchronized chaos [6], research on chaos dynamics has received considerable attention; particularly, in light of the potential application of this phenomenonin communication safety [7,8,9]. Data encryption using chaotic systems was reported in the 90´s as a new method to code and decode signals other than the conventional methods that use numerical algorithms as the encryption key [10]. The number of computer crimes has increased considerably. Safety in image broadcasting has become an important topic worldwide [11]. Image encryption schemes are being studied more and more due to the demand to find security in real-time image broadcasting through the Internet, as well as wireless networks [12,13]. Chaotic systems have important properties, such as: high sensitivity to the initial conditions [14], the property of pseudo-randomness, no periodicity, and the dependency of the system parameters. These properties are related to Shannon´s requirements for permutation and diffusion in cryptosystem building [15].

The DSK 5510 can be used for the implementation of Lorenz's system, Rössler system and Chua's circuit and other chaotic systems such as Logistic map, Henon map, Trigonometric map,etc.

2 Lorenz, Rössler and Chua's circuit chaotic systems

We considered the Lorenz system [1,5] given by equations:

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - xz - y \quad (1) \\ \dot{z} &= xy - bz \end{aligned}$$

It is well-known that with the parameter values $\sigma = 10$, $r = 28$, and $b = 8/3$Lorenz system exhibits chaotic dynamics [17]. Initial conditions of the system are: $(x(0), y(0), z(0)) = (3,15,1)$, Figure 1 shows the time series and their chaotic attractor is presented in Figure 2.

Rössler system[3] is given by equations:

$$\begin{aligned} \dot{x} &= -(y+z) \\ \dot{y} &= x + ay \\ \dot{z} &= b + xz - cz \end{aligned} \qquad (2)$$

Time series in MatLab for variables x, y and z of the Rössler system can be seen in Figure 3 and their attractor is shown in Figure 4.

Chua's oscillator is a third order autonomous system, which can be easily realized in electronic form [18] and exhibits a wide variety of nonlinear and chaotic phenomena. The dimensionless state equations [19] are given by:

$$\begin{aligned} \dot{x} &= \alpha(y - x - g(x)) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y - \gamma z, \\ g(x) &= cx + (1/2)(d-c)(|x+1| - |x-1|) \end{aligned} \qquad (2)$$

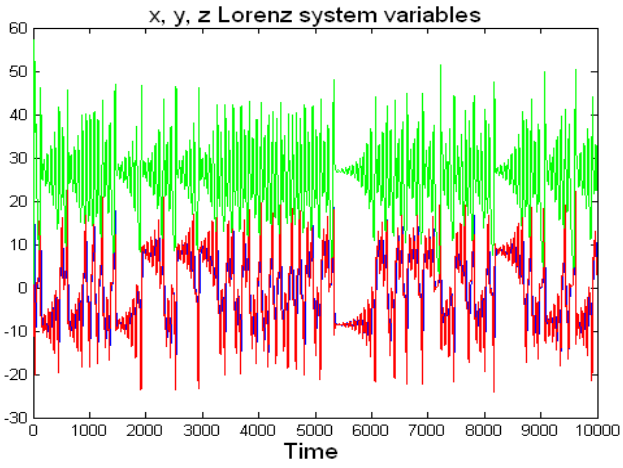

Figure 1. Time series in Lorenz system

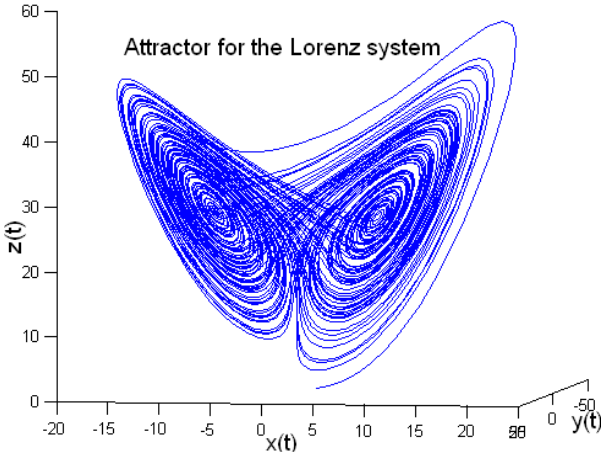

Figure 2. Attractor for the Lorenz system

Rössler system: the system shows a chaotic behavior for parameter's values, a = 0.2, b = 0.2, c = 6.3 and initial conditions x(0)=1, y(0)=1, z(0)=1. Figure 3 shows the time series and Figure 4 shows their chaotic attractor.

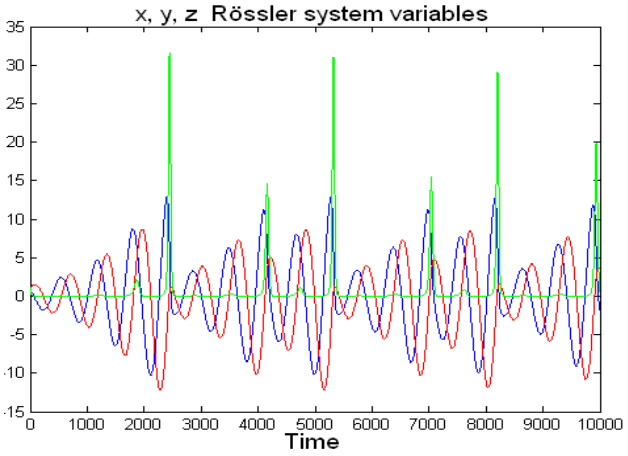

Figure 3. Time series in Rössler system

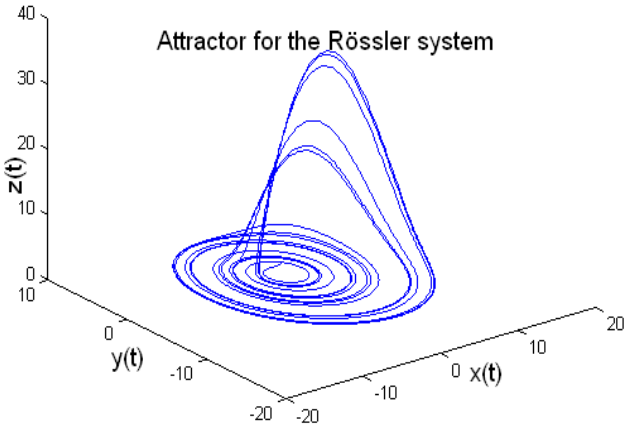

Figure 4. Attractor for the Rössler system

Chua's circuit: Δt=0.01, the dimensional parameters are: a = 15, b =25.58, and constants c =-0.7142857

and d = -1.142857; initial conditions x(0)=-1.6, y(0)=0, z(0)=1.6. Figure 5 and Figure 6 show the time series and their chaotic attractors respectively.

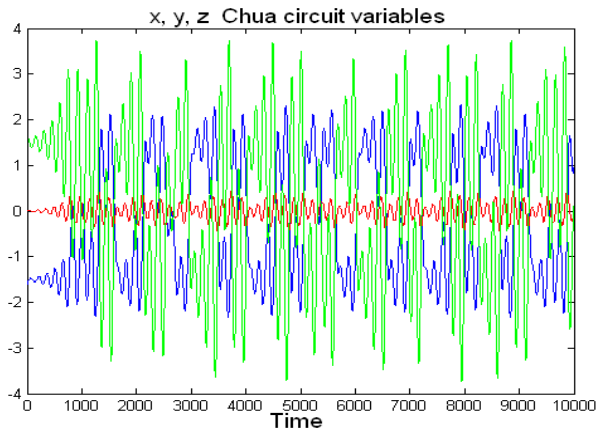

Figure 5. Time series in Chua's circuit

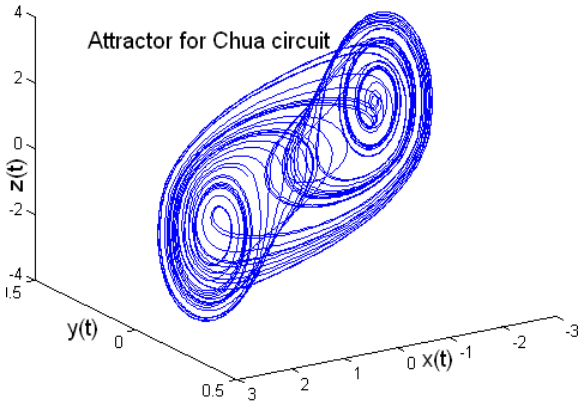

Figure 6. Attractor for Chua's circuit

3 Synthesis of the chaotic Lorenz system, Rössler system and Chua's circuit

To implement these chaotic systems, we use an approximation to the derivative by increments to convert the system of differential equations into a system of difference equations according to:

$\frac{\Delta y}{\Delta t} = \frac{y(k+1)-y(k)}{\Delta t}$, $\dot{x} = \sigma(y-x)$ became

$\frac{x(k+1)-x(k)}{\Delta t} = \sigma(y(k)-x(k))$ where

$x(k+1) = \Delta t[\sigma(y(k)-x(k))]+x(k)$.

In the same way the system of equations (1) results in:

$$\begin{aligned} x(k+1) &= \Delta t[\sigma(y(k)-x(k))]+x(k) \\ y(k+1) &= \Delta t[rx(k)-(x(k)*z(k))-y(k)]+y(k), \\ z(k+1) &= \Delta t[(x(k)*y(k))-bz(k)]+z(k) \end{aligned} \quad (4)$$

and the system of equations (2) results in:

$$\begin{aligned} x(k+1) &= \Delta t(-y(k)-z(k))+x(k) \\ y(k+1) &= \Delta t(-x(k)+ay(k))+y(k) \\ z(k+1) &= \Delta t(b+z(k)x(k)-cz(k)+z(k)) \end{aligned} \quad (5)$$

as well the system of equations (3) results in:

$$\begin{aligned} x(k+1) &= \Delta t(\alpha(y(i-1)-x(i-1)-(cx(i-1) \\ &+\frac{1}{2}(d-c)(|x(i-1)+1|-|x(i-1)-1|)))+x(i-1) \\ y(k+1) &= \Delta t(x(k)-y(k)+z(k))+y(k)+y(k) \\ z(k+1) &= \Delta t(-by(k))+z(k) \end{aligned} \quad (6)$$

4 Implementation of chaotic systems with DSP

The DSK features the TMS320C5510 DSP, a 200 MHz device delivering up to 400 million instructions per second (MIPs) [16], Other hardware features of the TMS320C5510 DSK board include: High-quality 24-bit stereo codec, 256K words of Flash and 8 MB SDRAM.

Simulations of the proposed chaotic oscillator systems were done using Matlab. To generate chaotic signals in real time we programmed a routine in C language that produced a frame of N samples, where each frame is sent to CODEC by mean of a double buffer system (Tic, Toc) Figure 7, at the same time the next sampling frame is being generated.

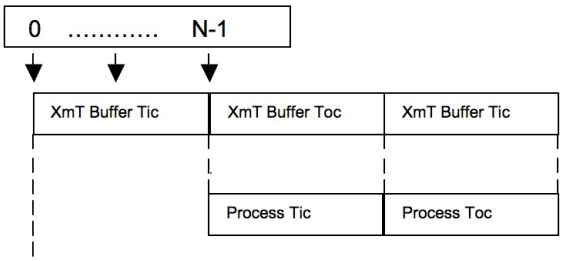

Figure 7. Double Buffer System Timing

The time required to send the N samples of the buffer to CODEC is the available time to produce (process) a new sampling frame of the signal as show in Figure 8. The proposed system is possible due to the characteristic of DMA (Direct Memory Access) and high performance of DSP in the processing and generation of the chaotic signal (Figure 9, Figure 10 and Figure 11).

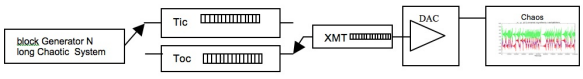

Figure 8. General diagram for the generation of chaotic signals with DSP´s

5 Experimental results

Time series for all variables in the three systems were obtained with the DSP in real time (Figure 9, Figure 10 and Figure 11). These results are consistent with the simulation results in MATLAB (differed time) Figure1, Figure 3, and Figure 5.

The sampling period, ΔT, is determined by the original chaotic equation, which is usually varied with different chaotic systems. For example, ΔT is selected as 0.01 for the Lorenz system, 0.05 for Rössler system and 0.011 for the Chua's circuit

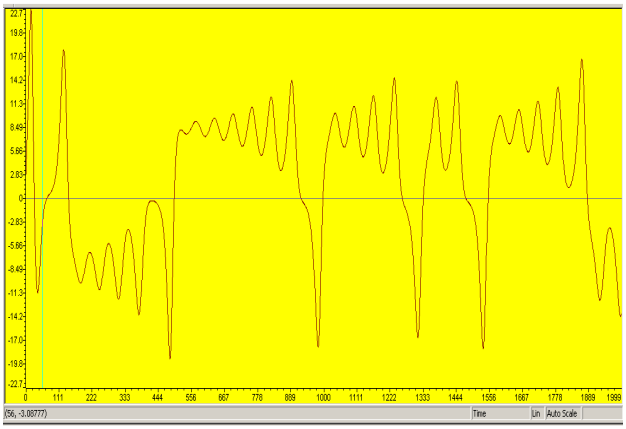

Figure 9. Time series in Lorenz system for the "x" variable

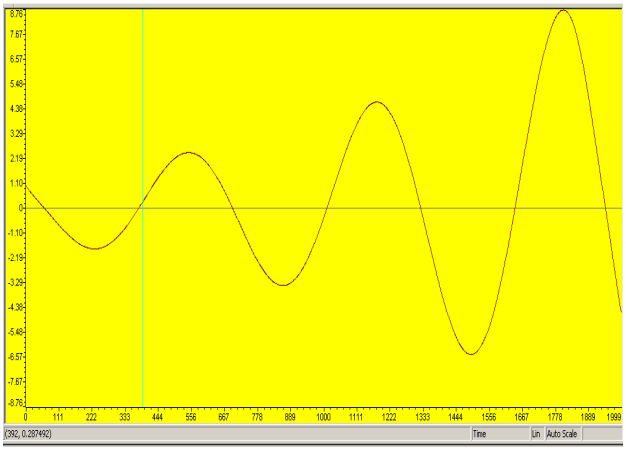

Figure 10. Time series in Rössler system for the "x" variable

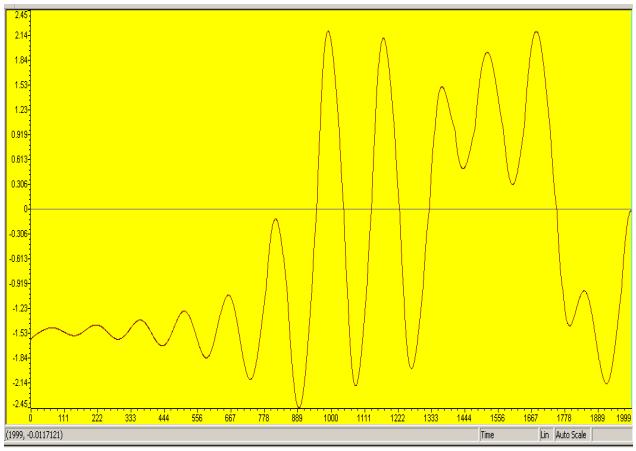

Figure 11. Time series in Chua's circuit for the "x" variable

Some of the benefits of using DSP are: processing time, FFT calculation, Liapunov coefficients, spectral analysis, phase diagrams …etc. A DSP system is robust and can easily adapt to any changes in parameters and variables and they can be reprogrammed. It is not necessary to change the hardware when a new system is required.

A digital signal processor (DSP) is a type of microprocessor - one that is incredibly fast and powerful [16]. A DSP is unique because it processes data in real time and this real-time capability makes a DSP perfect for applications where we won't tolerate any delays.

6 Conclusion

In this work, we present results of the implementation of chaotic generators with DSPs. They were programmed on "C" language and the main idea consists of the synthesis of chaotic generators using the DSK 5510 Texas instrument development card. The models of Lorenz system, Rössler system and Chua's circuit were used for this purpose. The DSK 5510 can be used for the implementation of all the other chaotic systems such as: Logistic map, Henon map, Trigonometric map, etc. as well as for image encryption

References:

[1] Lorenz E.N.,, Deterministic nonperiodic flow, *J. Atmosph, Sci.*, Vol.20, 1963,pp.130-141.

[2] Rössler O. E., An equation for continuous chaos, *Phys. Lett.*,Vol.57-A, number 5,1976, pp. 397-398.

[3] Stephen, Lynch, *Dynamical Systems with applications using matlab*, Birkhäuser, 2004.

[4] R.N. Madan, *Chua´s Circuit: A Paradigm for Chaos*, World Scientific, Singapore, 1993.

ISBN: 978-960-474-374-2

[5] Kevin M. Cuomo, Alan V. Oppenheim, and Steven H. Strogatz, "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications",*IEEE Transactions on Circuits and Systems, Analog and Digital Signal Processing*, Vol.40, No.10, 1993,pp 623-633.

[6] Pecora L.M. y Carroll T.L. Synchronization in chaotic systems, *Phys. Rev. Lett*.,Vol.64,1990, pp. 821-824.

[7] Alvarez G.,Li S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *Int. J.Bifurc. Chaos*, Vol.16, no. 8, 2006,pp. 2129-2151.

[8] Gámez G. L., Cruz Hernández. C., López Gutiérrez, R.M. García G.E.E. Synchronization of multi-scroll chaos generators: application to private communication. *Revista Mexicana de Física,*Vol.54(4),2008, pp. 299-305.

[9] Gámez G. L., Cruz Hernández. C., López Gutiérrez, R.M., García G.E.E. Synchronization of Chua'scircuits with multi-scroll Application to communication.. *Commun Nonlinear SciNumerSimulat,*Vol.14,2009, pp. 2765-2775.

[10] C. Cruz-Hernández, D., López-Mancilla V., García-Gradilla, H. Serrano-Guerrero and R. Nuñez-Pérez, Experimental realization of binary signals transmission using chaos. *Journal of Circuits,Systems and Computers,*Vol.14, 2005, pp. 453-468.

[11] LópezGutiérrez,.R. M., Posadas Castillo, C. LópezMancilla. D. Cruz Hernández, C. Communicating via robust synchronization of chaotic lasers. *Chaos, Solitons and Fractals,*Vol.42,2009,pp. 277-285.

[12] Chen G. R, Mao YB, et al.. A symmetric image encryption scheme based on 3D chaotic cat maps.*Chaos, Solitons and Fractals,*Vol.21, 2004, pp. 749–761.

[13] Chiaraluce F, Ciccarelli L, et al. A new chaotic algorithm for video encryption. *IEEE Trans ConsumElectron,*Vol.48, 2002, pp. 838–43.

[14] Ponomarenko, V.I. & Prokhorov, M. I. Extracting information masked by the chaotic signal of a time-delay system, *Phys. Rev. E,*Vol.66, 2002, pp. 026215.

[15] Li S., Alvarez G., and Chen G. Breaking a chaos-based secure communication scheme designed byan improved modulation method. *Chaos, Solitons and Fractals*, Vol.25, no. 1, 2005, pp. 109-120.

[16] Technical Reference websitehttp://focus.ti.com/docs/toolsw/folders/print/tmdsdsk5510.html,http://www.ti.com/corp/docs/investor/dsp/why.htm.

[17] D.López- Mancilla, C. Cruz-Hernandez,, and C. Posadas Castillo ,"A Modified Chaos-BasedComunication Scheme Using Hamiltonian Forms and Observer". *Journal of Physics: ConferenceSeries,*Vol.23, 2005, pp. 267-275.

[18] M.P. Kennedy, "Robust op amp realization of Chua's circuit,"*Frecuenz*, Vol.46, no.3-4,1992, pp. 66-80.

[19] Chai Wah Wu, Synchronization in Coupled Chaotic Circuits and Systems. *Word Scientific Series A*,Vol. A, Vol.41, 2002, pp.157-159