Adaptive Synchronization in Chaotic Secure Communication Systems Using Chua’s Circuit

Abolhassan Razminia, Kambiz Razminia, Alireza Nemati, Gholamreza Bazdar

Abstract**—** In this paper, some practical pilots of synchronization which are applied to a secure communication system are illustrated. An adaptive mechanism using Lyapunov technique is proposed to synchronize two practical Chua’s circuits in a secure communication system with a noisy environment and in the presence of unavoidable variations in the physical devices in actual implementation. The parameters of the circuit are considered fixed but unknown. Using the well-known Lyapunov technique, it is proven that the error between two signals from master and slave circuit converges to zero. The simulations show the effectiveness of the method.

Keywords**—** Chaotic Systems, secure communication systems, Lyapunov method, adaptive control, synchronization, Chua’s circuit.

I. Introduction

NOWADAYS secure communication has entered in the attractive and interesting research fields, either in digital communication systems or in the control theory. The avalanche of the paper depicts these importance and versatility [1]. As a main application of this field one can see the papers published in the journals related to military industries [2]. Coding is the heart of a military system which if is mixed with the chaotic signals can be more secure than the usual coding algorithms [3].

An important field in the modern digital communication systems is chaotic modulation which is increasingly used in the military industries and coding blocks because of its preference in security and safety against the forbidden users. One of the most important tasks in practical implementation of these technologies is synchronization between the carrier signal in the transmitter and receiver. Chua’s circuit has been mainly used in the generation of chaotic signals and synchronization strategies**.**

In recent years, there has been explosive growth in personal communications, the aim of which is to guarantee the availability of voice and/or data services between mobile communications terminals. In order to provide these services, radio links are required for a large number of compact terminals in densely populated areas. As a result, there is a need to provide high-frequency, low-power, and low-voltage circuitry [4]. The huge demand for telecommunications results in a large number of users; therefore, today's telecommunications systems are limited primarily by interference from other users. In some applications, the efficient use of available bandwidth is extremely important, but in other applications, where the exploitation of communication channels is relatively low, a wideband communication technique having limited bandwidth efficiency can also be used [5].

Often, many users must be provided with simultaneous access to the same or neighboring frequency bands. The optimum strategy in this situation, where every user appears as interference to every other user, is for each communicator's signal to look like white noise which is as wideband as possible [5].

There are two ways in which a communicator's signal can be made to appear like wideband noise:

1. by spreading each symbol using a *pseudorandom* sequence to increase the bandwidth of the transmitted signal, or
2. by representing each symbol by a piece of *noise-like* waveform.

The conventional solution to this problem is the first approach: to use a synchronizable pseudorandom sequence to spread the transmitted signal and to use a conventional modulation scheme based on phase shift keying (PSK) or frequency shift keying (FSK) [6].

Such direct sequence spread spectrum (SS) schemes have processing gain associated with dispreading at the receiver, and the possibility to provide multiple access by assigning mutually orthogonal sequences to different users. This is the basis of code division multiple access (CDMA) communications systems [7]. Limitations are imposed by the need to achieve and maintain carrier and symbol synchronization, by the periodic nature of the spreading sequences, the limited number of available orthogonal sequences, and the periodic nature of the carrier. One further problem is that the orthogonality of the spreading sequences requires the synchronization of all spreading sequences used

Corresponding author; Abolhassan Razminia is a Ph.D. student of Control Engineering Department, Tarbiat Modares University, Tehran, Iran. Email: razminia@modares.ac.ir. & a.razminia@gmail.com.
Kambiz Razminia received his Bs degree from Petroleum Engineering University, Ahwaz, Iran. Email: kambiz.razminia@gmail.com.
Alireza Nemati received his M.Sc. degree from Shahrood University of Technology, Shahrood, Iran. Email: Nem_alireza@yahoo.ca.
Gholamreza Bazdar received his M.Sc. degree from Imam Hossein, Tehran, Iran. Email: g.bazdar@gmail.com.

in the same frequency band, i.e. the whole system must be synchronized. Due to different propagation times for different users, perfect synchronization can never be achieved in real systems.

An alternative approach to making a transmission noise-like is to represent the transmitted symbols not as weighted sums of periodic basis functions but as inherently non-periodic chaotic basis functions [8].

A Historical View on Chuas's Circuit

The chaotic nature of Chua's circuit was first observed by Matsumoto in 1983 using computer simulations, following the instructions of Chua, who had invented this circuit and had explained its operating principles to Matsumoto moments before he was rushed to a hospital for a major surgery, and who did not participate in the early phases of this research. In acknowledging his subsidiary role as a computer programmer, Matsumoto had named this circuit Chua's circuit.

The first experimental Chua's circuit which confirms the presence of chaos was due to Zhong and Ayrom in 1984. A second experimental circuit was reported by Matsumoto and was designed by Tokunaga, who is also responsible for obtaining all of the experimental result presented in that paper. The global bifurcation landscape of Chua's circuit was obtained by Komuro and a team of students of Matsumoto.

The first rigorous proof of the chaotic nature of Chua's circuit was given in 1986 [19], where the authors proved that there exists some parameters (α,β) such that Chua's circuit satisfies Shil'nikov's theorem and, therefore, has infinitely many Horseshoe maps.

Inspired by a question posed by professor J. Neirynck in 1991 on whether this canonical circuit is unique, a systematic search has since been completed by several researchers, including A. Huang and Lj.Kocarev, where many more distinct canonical circuits has been found.

II. Chaos Theory and Chaotic Carriers

Deterministic dynamical systems are those whose states change with time in a deterministic way. They may be described mathematically by differential or difference equations, depending on whether they evolve in continuous or discrete time [9]. Deterministic dynamical systems can produce a number of different steady-state behaviors including *equilibria, periodic,* and *chaotic solutions* [10]. *Equilibrium* is a non-oscillatory state. *Periodic* behavior is the simplest type of steady-state oscillatory motion. Sinusoidal signals, which are universally used as carriers in analog and digital communications systems, are periodic solutions of continuous- time deterministic dynamical systems.

Deterministic dynamical systems also admit a class of non periodic signals which are characterized by a continuous noise-like broad power spectrum; this is chaos [11]. In the time domain, chaotic signals appear random. Chaotic systems are characterized by super-sensitive dependence on initial conditions; a small perturbation eventually causes a large change in the state of the system [10]. Figure 1 shows this phenomenon for a chaotic Chua's system [12].

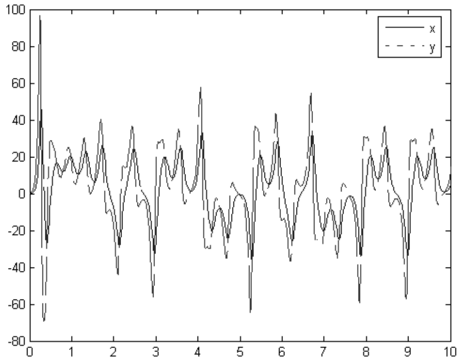

Figure 1. Super-sensitivity to initial conditions in a chaotic Chua system.

Equivalently, chaotic signals diverge rapidly with themselves. The autocorrelation function of a chaotic signal has a large peak at zero and decays rapidly [13]. Thus, while chaotic systems share many of the properties of stochastic processes, they also possess a deterministic structure which makes it possible to generate noise-like chaotic signals in a theoretically reproducible manner. In particular, continuous time chaotic systems can be used to generate wideband carriers, i.e. basis functions for chaotic digital communications systems [3].

It is shown that the use of sinusoidal signals as basis functions in conventional digital modulation techniques offers excellent bandwidth efficiency [14].

Moreover, these basis functions can be reconstructed easily by recovering a single sinusoidal carrier at the receiver. Why, then, is it necessary even to consider a modulation scheme which uses anything other than a sinusoidal carrier?

When a sinusoidal carrier is used, the transmitted power is concentrated in a narrow band, thereby resulting in high power spectral density. This has a number of serious drawbacks.

1. Multipath propagation is always present in many important radio applications such as mobile telephony and wireless LAN. It results in very high attenuation over narrow frequency bands. This means that the SNR may become very low or even a dropout may occur in a narrowband communications system. *Low SNR results in symbol errors due to the cycle slips in the carrier recovery circuit.* The extremely high attenuation causes not only a dropout in reception, but also loss of synchronization. Recall that *when synchronization is lost in a coherent receiver, all symbols transmitted during the pull-in time of the receiver's synchronization circuitry are also lost.*
2. Due to the high transmitted power spectral density, narrowband communications cause high levels of interference with other users. Therefore, they are not suitable for unlicensed radio applications.

3. Narrowband signals are sensitive to narrowband interference.
4. Because of the high transmitted power spectral density, the probability of interception of narrowband communications is high.
5. The reception of messages by an unauthorized receiver is very simple because limited a priori knowledge is required for demodulation.

The difficulties summarized above can be overcome by using spread-spectrum (SS) techniques, where, in addition to a conventional digital modulation scheme, a pseudorandom spreading sequence is used to spread the spectrum of the transmitted signal [4]. *The benefits of spreading can be achieved only if the pseudorandom sequences in the transmitter and receiver are synchronized*. This is our motivation for proposing an adaptive technique in this paper.

Spread-spectrum communications using spreading sequences has two major disadvantages:

1. It is not possible to achieve and maintain synchronization under poor propagation conditions,
2. The spreading and despreading processes require additional circuitry.

Chaotic signals are wideband signals that can be generated using very simple circuitry, e.g. Chua's circuit. A potentially cost-effective solution for wideband communications is to use a wideband chaotic carrier. In this approach, sample functions of chaotic waveforms are used as basis functions or as the elements of the signal set.

A. *Secure Communications*

The basic idea of digital secure communication using a chaotic carrier is that the bits (binary modulation) or symbols (*M*-ary modulation) are mapped to sample functions of chaotic signals emanating from one or more chaotic attractors [15]. In order to avoid periodicity, the symbols are mapped to the actual non-periodic outputs of chaotic circuits and not to parameters of certain known sample functions [16].

The principle difference between a chaotic carrier and a conventional periodic carrier is that the sample function for a given symbol is non-periodic and is different from one symbol interval to the next. Thus, the transmitted waveform is never periodic, even if the same symbol is transmitted repeatedly.

As in the case of conventional digital communications, we have four categories of modulation techniques [3]:

- *coherent correlation receiver with chaotic synchronization*;
- *coherent matched filter receiver*;
- *noncoherent detection techniques*;
- *differentially coherent reception*.

III. Chua's Circuit

A. *Fundamental Discussions*

The Chua's circuit, a third-order autonomous, dissipative electrical circuit, has been investigated thoroughly at the experimental, numerical and analytical levels [17]. This circuit, known for its rich repertoire of nonlinear dynamical phenomena and has become a universal paradigm for chaos [18]. We simulate this circuit in EWB space as shown in Figure 2.

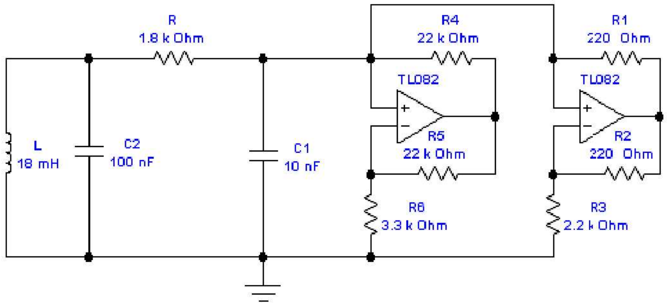

Figure 2. Chua's circuit simulated via EWB.

The equations that discuss the dynamics of this circuit is as follows:

$$\begin{cases} C_2\dot{v}_2 = \dfrac{1}{R}(v_1 - v_2) + i_3 \\ C_1\dot{v}_1 = \dfrac{1}{R}(v_1 - v_2) - f(v_1) \\ L\dot{i}_3 = -v_2 \end{cases} \tag{1}$$

In which v_1, v_2, i_3 are the voltages across capacitors C_1, C_2 and the current through the inductor L respectively. Also the nonlinear function $f(v_1)$ has the following characteristic:

$$f(v_1) = m_0 v_R + \frac{1}{2}(m_1 - m_0)\{|V_R + B_P| - |v_R - B_P|\} \tag{2}$$

Running this file in EWB space, one can have seen the phase portrait of the voltages of the capacitors versus each other. This is brought in Figure 3 which is a practical observation on an oscilloscope.

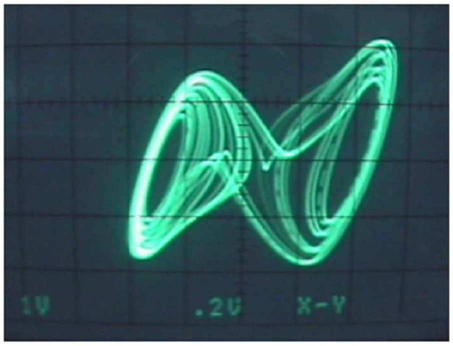

Figure 3. Phase portrait of the voltages of the circuit against each other.

B. A setup designed for experiment

For our experimental study we design a simple transceiver using elementary electronic devices. Figure 4 shows this circuit in detail.

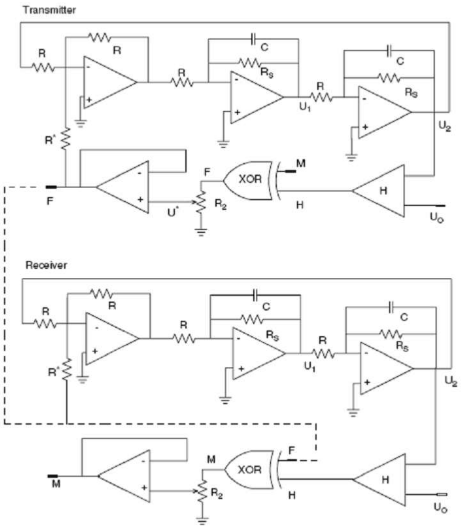

Figure 4. A transceiver designed for the experimental setup.

IV. Adaptive Synchronization of Two Chua's Circuit in the Pilot Setup

Consider two Chua's circuit as the transceiver in the secure communication pilot. The goal of this paper is to introduce an adaptive mechanism that synchronizes these two circuits. In other words we want to design a controller such that the output signals of the two circuits namely, drive circuit and response circuit, converge to each other asymptotically. Infact the output signal of the drive circuit is reference that the output of the response circuit must move towards it.

Now suppose the two circuits used in the source and destination are similar. The only difference is in their initial conditions. This may produce dangerous results if the synchronization circuit was not designed suitably.

After a simple parameter variation in (1) we write the equations describe the drive circuit with index D:

$$\begin{cases} \dot v_{1D} = \alpha(v_{1D} - v_{2D}) - \lambda f(v_{1D}) \\ \dot v_{2D} = \beta(v_{1D} - v_{2D}) + \delta i_{3D} \\ \dot i_{3D} = -\sigma v_{2D} \end{cases} \tag{3}$$

And the response circuit equations are as follows:

$$\begin{cases} \dot v_{1R} = \alpha(v_{1R} - v_{2R}) - \lambda f(v_{1R}) \\ \dot v_{2R} = \beta(v_{1R} - v_{2R}) + \delta i_{3R} \\ \dot i_{3R} = -\sigma v_{2R} \end{cases} \tag{4}$$

Note that the main assumption is the similarity between the parameters of the drive and response systems.

Defining the errors:

$$\begin{cases} e_1 = v_{1R} - v_{1D} \\ e_2 = v_{2R} - v_{1D} \\ e_3 = i_{3R} - i_{3D} \end{cases} \tag{5}$$

For finding the error dynamic one can differentiate these relations with respect to time:

$$\begin{cases} \dot e_1 = \alpha(e_1 - e_2) - \lambda(f(v_{1R}) - f(v_{1D})) + u_1 \\ \dot e_2 = \beta(e_1 - e_2) + \delta e_3 + u_2 \\ \dot e_3 = -\sigma e_2 + u_3 \end{cases} \tag{6}$$

Here u_1, u_2, u_3 are the control signals. Here we impose a constraint on the system parameters. They are constant but unknown. In this case for utilizing the well-known Lyapunov technique [20] we should use the estimated versions of those parameters. In what follows the hat parameter is the estimated parameter, e.g. $\hat\alpha$ is the estimated version of α .

The structure of the controller is proposed as follows:

$$\begin{cases} u_1 = \hat\alpha(e_2 - e_1) - \hat\lambda(f(v_{1D}) - f(v_{1R})) + Ae_1 \\ u_2 = \hat\beta(e_2 - e_1) - \hat\delta e_3 + Be_2 \\ u_3 = \hat\sigma e_2 + Ce_3 \end{cases} \tag{7}$$

Now define the estimation error:

$$\begin{cases} \tilde\alpha = \alpha - \hat\alpha \\ \tilde\beta = \beta - \hat\beta \\ \tilde\lambda = \lambda - \hat\lambda \\ \tilde\delta = \delta - \hat\delta \\ \tilde\sigma = \sigma - \hat\sigma \end{cases} \tag{8}$$

Consider the following Lyapunov function:

$$V = \frac{1}{2}[e^T e + \tilde\alpha^2 + \tilde\beta^2 + \tilde\lambda^2 + \tilde\delta^2 + \tilde\sigma^2] \tag{9}$$

Direct differentiation of this function respect to time along the system trajectories we have:

$$\dot V = e^T \dot e + \tilde\alpha\dot{\tilde\alpha} + \tilde\beta\dot{\tilde\beta} + \tilde\lambda\dot{\tilde\lambda} + \tilde\delta\dot{\tilde\delta} + \tilde\sigma\dot{\tilde\sigma} \tag{10}$$

In which:

$$\begin{cases} e_1\dot{e}_1 = e_1(e_1 - e_2)\tilde{\alpha} - e_1(f(v_{1R}) - f(v_{1D}))\tilde{\lambda} + Ae_1{}^2 \\ e_2\dot{e}_2 = e_2(e_1 - e_2)\tilde{\beta} + e_2 e_3\tilde{\delta} + Be_2{}^2 \\ e_3\dot{e}_3 = -e_2 e_3\tilde{\sigma} + Ce_3{}^2 \end{cases} \qquad (11)$$

Now we consider the adaptation law as follows:

$$\begin{cases} \dot{\tilde{\alpha}} = e_1(e_2 - e_1) \\ \dot{\tilde{\beta}} = e_2(e_2 - e_1) \\ \dot{\tilde{\lambda}} = e_1(f(v_{1R}) - f(v_{1D})) \\ \dot{\tilde{\delta}} = -e_2 e_3 \\ \dot{\tilde{\sigma}} = e_2 e_3 \end{cases} \qquad (12)$$

Using these laws we can easily find the simple form of $\dot{V}$ as follows:

$$\dot{V} = Ae_1{}^2 + Be_2{}^2 + Ce_3{}^2 \qquad (13)$$

In which the three parameters A, B, C are free and we must choose them so that $\dot{V} \le 0$. For example we can choose: $A = B = C = -1$. In this case, it is guaranteed that the error vector tends to zero asymptotically. This means that the outputs of the drive and response circuits are synchronized.

Figure 6 shows the synchronization between the currents of the inductors of drive and response circuits. Figure 7 and 8 shows the synchronization between corresponding voltages in drive and response circuits. These simulations show the effectiveness of the propose method clearly.

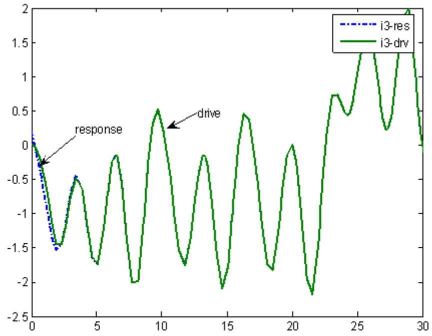

Figure 5. Synchronization between currents of the master and slave circuits.

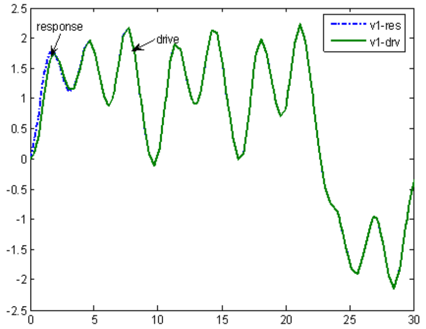

Figure 6. Synchronization between voltages of capacitors 1.

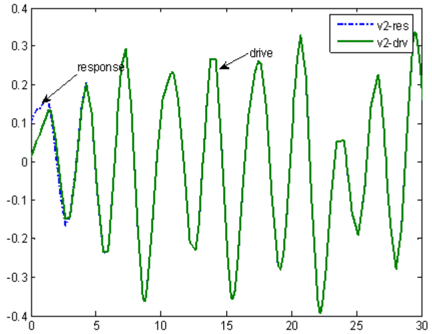

Figure 9. Synchronization between voltages of capacitors 2.

V. Conclusion

In this paper we review some important point in the secure communication and the problems arising in the synchronization strategies. Some remarks are discussed about why we use the chaotic carriers instead of sinusoidal ones. The well-known Chua's circuit was surveyed. As our main contribution using Lyapunov technique an adaptive mechanism is proposed which the simulations highlight the ability of the method. As we mentioned above according to super-sensitivity to initial conditions as the main feature of the chaotic systems, a slight difference between the initial conditions in the drive circuit in the transmitter and the response circuit in the receiver can deteriorate the synchronization if the carrier signal is chaotic. Thus a robust property is injected to the synchronization algorithm based on the adaptive methodology. As an open problem one can try to solve the problem in the case that the parameters of the drive and response are not similar.

References

[1] B.R. Andrievskii, and A.L.Fradkov, " Control of chaos: Methods and applications. I. Methods", Avtom.Telemkh, no. 5, pp.3-45. 2003.

[2] A. Jameel, M.Y. Siyal, N. Ikram, “A robust secure speech communication system using ITU-T G.723.1 and TMS320C6711 DSP”, Microprocessors and Microsystems, Volume 30, Issue 1, 1 February 2006, Pages 26-32.

[3] Wei-Der Chang, “Digital secure communication via chaotic systems”, Digital Signal Processing, Volume 19, Issue 4, July 2009, Pages 693-699.

[4] Jing Dong, Kurt Ackermann, Cristina Nita-Rotaru, “Secure group communication in wireless mesh networks”, Ad Hoc Networks, In Press, Corrected Proof, Available online 12 April 2009.

[5] Jeffrey E. Wieselthier, Gam D. Nguyen, Anthony Ephremides, “Resource management in energy-limited, bandwidth-limited, transceiver-limited wireless networks for session-based multicasting”, Computer Networks, Volume 39, Issue 2, 5 June 2002, Pages 113-131.

[6] J. Thoné, S. Radiom, D. Turgis, R. Carta, G. Gielen, R. Puers, “Design of a 2 Mbps FSK near-field transmitter for wireless capsule endoscopy”, Sensors and Actuators A: Physical, In Press, Corrected Proof, Available online 11 December 2008.

[7] Fang-Biau Ueng, Hsuan-Fu Wang, Jui-Chi Chang, “Convergence analysis of adaptive DS-CDMA receivers in multi-path channels”, Signal Processing, Volume 89, Issue 4, April 2009, Pages 438-449.

[8] Changchun Hua, Bo Yang, Gaoxiang Ouyang, Xinping Guan, “A new chaotic secure communication scheme”, Physics Letters A, Volume 342, Issue 4, 18 July 2005, Pages 305-308.

[9] Ling Hou, Anthony N. Michel, “Unifying theory for stability of continuous, discontinuous, and discrete-time dynamical systems”, Nonlinear Analysis: Hybrid Systems, Volume 1, Issue 2, June 2007, Pages 154-172.

[10] Nikolai A. Magnitskii, “Universal theory of dynamical chaos in nonlinear dissipative systems of differential equations”, Communications in Nonlinear Science and Numerical Simulation, Volume 13, Issue 2, March 2008, Pages 416-433.

[11] Xiang Yu, Shijian Zhu, Shuyong Liu, “A new method for line spectra reduction similar to generalized synchronization of chaos”, Journal of Sound and Vibration, Volume 306, Issues 3-5, 9 October 2007, Pages 835-848.

[12] Hinke M. Osinga, Bernd Krauskopf, “Visualizing the structure of chaos in the Lorenz system”, Computers & Graphics, Volume 26, Issue 5, October 2002, Pages 815-823.

[13] V. S. Anishchenko, T. E. Vadivasova, G. A. Okrokvertskhov, G. I. Strelkova, “Correlation analysis of dynamical chaos”, Physica A: Statistical Mechanics and its Applications, Volume 325, Issues 1-2, 1 July 2003, Pages 199-212.

[14] G.K. Singh, “A research survey of induction motor operation with non-sinusoidal supply wave forms”, Electric Power Systems Research, Volume 75, Issues 2-3, August 2005, Pages 200-213.

[15] Jui-Sheng Lin, Cheng-Fang Huang, Teh-Lu Liao, Jun-Juh Yan, “Design and implementation of digital secure communication based on synchronized chaotic systems”, Digital Signal Processing, In Press, Corrected Proof, Available online 4 May 2009.

[16] A. Gálvez, A. Iglesias, “Symbolic/numeric analysis of chaotic synchronization with a CAS”, Future Generation Computer Systems, Volume 23, Issue 5, June 2007, Pages 727-733.

[17] L. Gámez-Guzmán, C. Cruz-Hernández, R.M. López-Gutiérrez, E.E. García-Guerrero, “Synchronization of Chua’s circuits with multi-scroll attractors: Application to communication”, Communications in Nonlinear Science and Numerical Simulation, Volume 14, Issue 6, June 2009, Pages 2765-2775.

[18] Jinzhi Wang, Zhisheng Duan, Lin Huang, “Dichotomy of nonlinear systems: Application to chaos control of nonlinear electronic circuit”, Physics Letters A, Volume 351, Issue 3, 27 February 2006, Pages 143-152.

[19] Arnold Neumaier, Thomas Rage, “Rigorous chaos verification in discrete dynamical systems”, Physica D: Nonlinear Phenomena, Volume 67, Issue 4, 1 September 1993, Pages 327-346.

[20] Q. Wu, N. Sepehri, P. Sekhavat, S. Peles, “On design of continuous Lyapunov's feedback control”, Journal of the Franklin Institute, Volume 342, Issue 6, September 2005, Pages 702-723.