A New Nonlinear Chua's Chaotic Structure System for Information Cipher Applications

You-Yu Jan
Department of Electronic Engineering, Ching-Yun University; Master degree student
e-mail：m9411018@cyu.edu.tw

Yuan-Fong Chau
Department of Electronic Engineering, Ching-Yun University; Assistant Professor
e-mail：yfc01@cyu.edu.tw

Yuh-Sien Sun
Department of Electronic Engineering, Ching-Yun University; Assistant Professor
e-mail：sunys@cyu.edu.tw

Abstract

In this paper, we propose a new nonlinear Chua's chaotic structure cipher system. This new nonlinear cipher system can be used to enhance the original Chua's circuit chaotic nonlinear performance. This new chaotic cipher system is shown workable and it's effective chaotic parameters range is depicted and proposed also. This chaotic based cipher scheme can be applied on a one-time pad approached applications.

Keywords：Chua's circuit, chaotic system, cipher system, parameter range.

摘要

本篇論文中，我們提出一種新型非線性蔡氏混沌結構加密系統。此一新型非線性加密系統能被用來強化原始蔡氏電路混沌系統非線性的特性。此一新的混沌加密系統經本文的推導證明是可運作的且其參數群的個別有效混沌特性的範圍亦被建議指出。此一以混沌為基礎的加密微分方程系統能被運用於近似一次密的多種應用中。

關鍵詞：蔡氏電路、混沌系統、加密系統、參數範圍。

1. Introduction

In the past few years various nonlinear electronic systems which show chaotic behavior have been constructed and described theoretically [1,3,8,9,11,12]. Certain effects blamed on noise are really examples of chaotic behavior of a completely deterministic nature. Chaotic dynamics have been successfully exploited in communication applications, and these include chaotic encryption for security, and chaotic modulation for the transmission of analog and digital information [1]. One such circuit is Chua's circuit which is a third order RLC circuit with four linear elements (two capacitors, one resistor and one inductor), and has only one piecewise linear resistor for approaching the nonlinear phenomena. Chaotic circuits and their applications to secure communications have received a great deal of attention since Pecora and Carrol proposed a method to synchronize two identical chaotic systems [11]. The main advantage of a chaotic secure communication system over conventional cryptosystems is that chaotic secure communication systems can often be realized as very simple circuits (or emulated digital software) on a part of a chip. The primary aim of this paper is to enhance the piece wise linear to real nonlinear domain to secure the nonlinear depth of Chua's chaotic system. Specifically, we introduce a sin nonlinear term to add on the piece wise linear curve, which can be used to enlarge the nonlinear range of the chaotic cryptosystem and synchronization time is almost the same. The impulsive control strategy proposed in [5,6,7] is adopted to synchronize two identical chaotic systems embedded in the encoder and the decoder where the lengths of impulsive intervals are piecewise constant. The security of chaotic secure communication systems is further improved. Moreover, with the given parameters of chaotic system, estimate of the synchronization time is predictable.

The organization of this paper is as follows.

In Section 2, we propose a novel nonlinear digital chaotic system. The synchronization error issue is considered in Section 3. In Section 4, depicts some experimental results to illustrate this new nonlinear chaotic system are provided. Finally, some concluding remarks are presented in Section 5.

2. The Novel Nonlinear Digital Chaotic System

In this section, we shall present a novel nonlinear chaotic secure communication system that uses a magnifying glass to enlarge the effect of parameter mismatch and an impulsive control strategy [5,6,7] for the synchronization of chaotic circuits. The proposed scheme is essentially a one time pad with the random signal replaced by a chaotic signal generated from a nonlinear Chua's digital differential equations (1). This nonlinear chaotic cryptosystem is mainly composed of cipher transceivers. The input of system can be any types of signals which can be digitized into binary storage devices.

The cipher transceiver consists of a classical encrypt/decrypt function with the same digitized Chua's emulated differential equations. The cipher receiver side is added on an impulsive controller to fast tracking the same chaotic parameters. The function of impulsive controller is to synchronize Chua's equation which is embedded in the cipher transceiver. The key signal is a combination of all three state variables of the Chua's emulated differential equation circuit. The cipher text is obtained from the finite state machine XOR operation on the plaintext sequence bit by bit. The decryption is the same as the encryption, including the XOR operation of the transmitted scrambled signal. When the Chua's equivalent emulated differential equations in the cipher machine are synchronized, the cipher receiver can find the same key signal sequence as in the cipher transmitter to recovery the original plaintext bit sequence. For the cipher transmitter side, the dimensionless state equations of Chua's circuit are given [3] as

$$\begin{cases} \dfrac{dx_1}{dt} = k\alpha\left(x_2 - x_1 - f(x_1)\right) \\ \dfrac{dx_2}{dt} = k(x_1 - x_2 + x_3) \\ \dfrac{dx_3}{dt} = k(-\beta x_2 - \gamma x_3) \end{cases} \quad (1)$$

where α , β and γ are constants, $k \in [-1,1]$ and the $f(x)$ is our proposed the novel nonlinear function of Chua's chaotic which is added on a nonlinear curve of digital Sin term to improve the original piecewise linear phenomena, which is given as

$$f(x) = bx + \frac{1}{2}(a-b)\{|x+1| - |x-1|\} - 0.05\sin(x) \quad (2)$$

Where a and b are two negative constants. This $-0.05\sin(x)$ is a new added term. The 0.05 is a heuristic result and control the nonlinear response amplitude. The –sin(x) is used to tune and fit the slop curve of original piecewise linear to non-piecewise linear. Since the signals are transmitted through a digital channel, the synchronization issue should be quantized by a predefined quantize first, which depends on the amplification factor K . The quantization error should be less than certain values to ensure that the cipher transmitter and the cipher receiver can be synchronized. To provide the desired sequence, a magnifying term is introduced, which is composed of an amplifier and an observer. They are given the root mean square versus amplifying value as below:

The amplifier $k'(t) = K\left(x_1^2(t) + x_2^2(t) + x_3^2(t)\right)^{0.5}$, and the observer $k(t) = \left(\lfloor k'(t) \rfloor + \lambda\right) \bmod(\Omega)$, K is a given amplifying value and $\bmod(\Omega)$ is the finite field operator which is chosen to influence the sensitivity of the system, λ is an arbitrary integer and $\lfloor m \rfloor$ is the integer truncation of m . Therefore the scrambled signal v_R can be given by

$$v_R(t) = E(p(t)) = p(t) \oplus k(t) \quad (3)$$

where $p(t)$ is the plaintext, $k(t)$ is the observer, $E(p(t))$ is the cipher text, and $\oplus$ denotes XOR operator. For the cipher receiver side, the cipher receiver are given by

$$\begin{cases} \dfrac{d\tilde{x}_1}{dt} = k\alpha(\tilde{x}_2 - \tilde{x}_1 - f(\tilde{x}_1)) \\ \dfrac{d\tilde{x}_2}{dt} = k(\tilde{x}_1 - \tilde{x}_2 + \tilde{x}_3), \qquad t \neq \tau_n; n = 1,2,\cdots \\ \dfrac{d\tilde{x}_3}{dt} = k(-\beta\tilde{x}_2 - \gamma\tilde{x}_3) \end{cases} \quad (4)$$

and

$$\begin{bmatrix} \tilde{x}_1(\tau_n^+) \\ \tilde{x}_2(\tau_n^+) \\ \tilde{x}_3(\tau_n^+) \end{bmatrix} = \begin{bmatrix} \tilde{x}_1(\tau_n) \\ \tilde{x}_2(\tau_n) \\ \tilde{x}_3(\tau_n) \end{bmatrix}_{n=1,2,\cdots} - B \begin{bmatrix} Q(x_1(\tau_n^+)) - \tilde{x}_1(\tau_n) \\ Q(x_2(\tau_n^+)) - \tilde{x}_2(\tau_n) \\ Q(x_3(\tau_n^+)) - \tilde{x}_3(\tau_n) \end{bmatrix} \quad (5)$$

where B is a 3×3 matrix to be designed to satisfy certain inequality. Assume the $Q(\cdot)$ is a predefined quantize, and the times τ_n ; $\{\tau_n\}, 1 \le n \le \infty$, satisfy $0 < \tau_1 < \tau_2 < \cdots < \tau_n < \tau_{n+1} < \cdots$, $\tau_n \to \infty$ as $n \to \infty$, and $\tau_1 - \tau_0 = \tau_3 - \tau_2 = \cdots = \tau_{2i+1} - \tau_{2i} = \cdots$ Let $\Delta_1 = (\tau_{2i} - \tau_{2i-1})$ and $\Delta_2 = (\tau_{2i+1} - \tau_{2i})$. Δ_1 and Δ_2 satisfy that $\Delta_2 = \varepsilon_1\Delta_1$. Where ε_1 is an arbitrary number. The parameter of ε_1 is usually determined by the parameters of Chua's circuit. Typically set the $\varepsilon_1 = (|\alpha/\beta|)$. The matrix B and Δ_1 are chosen to synchronize the two chaotic systems (1) and (4) in the transmitter and the receiver, respectively. We denote the linear part of the system matrix of (1) and (4) as

$$A = \begin{bmatrix} -k\alpha & k\alpha & 0 \\ k & -k & k \\ 0 & -k\beta & -k\gamma \end{bmatrix} \quad (6)$$

Then B and Δ_1 are chosen according to the requirement of impulsive control strategy to satisfy the condition as below [6].

$$0 \le \nu + 2|\alpha a| \le -\frac{2}{(1+\varepsilon_1)\Delta_1}\ln(\xi d_1) \quad (7)$$

where $\xi > 1$, ν is determinate by the largest eigenvalue of $(A + A^T)$ and d_1 is the largest eigenvalue of $(I+B)^T(I+B)$. It has been shown by Theorem 2 of [6] that the chaotic systems proposed in the cipher transmitter and the cipher receiver are globally synchronized. Therefore, the cipher receiver received the plaintext and recovered via $\tilde{k}(t) = \left(\left\lfloor K\left(\tilde{x}_1^2((t) + \tilde{x}_2^2(t) + \tilde{x}_3^2(t)\right)^{0.5}\right\rfloor + \lambda\right) \bmod(\Omega)$, and

$$\tilde{p}(t) = \tilde{E}(p(t)) = \nu_R(t) \oplus \tilde{k}(t) \quad (8)$$

where $\tilde{E}(p(t))$ is the recovered encrypted signal. $\tilde{k}(t)$ is the recovered in the receiver circuit and should be approximate the $k(t)$. From (3) and (8), the original signal can be recovered only when two identical chaotic circuits in both the cipher transmitter and the cipher receiver are synchronized. Similarly, an intruder can know the original message only when he knows the parameters and the structure of the circuits and the synchronization impulses. In this situation, the system introduced a magnify term and the non-piecewise linear of sin term to transfer the chaotic state variables which act as key sequence before XOR with the plaintext. Assuming that there is a small mismatch that results in perturbation of $\Delta x_i(t) = \sigma_i (i = 1,2,3)$, then the signal getting through the amplifier has $k(t) = (\lfloor K(\sum_{i=1}^{3}(x_i(t) + \sigma_i)^2)^{0.5}\rfloor + \lambda) \bmod(\Omega)$.

Since the parameter K is a large number, we can see that the signal is enlarged many times, which implied that the parameters mismatch can be enlarged. And the sin(x) term also. Thus even a minor mismatch in the parameters will produce a large decryption error, resulting in a decryption key sequence that is not the same as the encryption key signal. So, the intruder cannot recover the original plaintext signal. The security of this nonlinear chaotic communication cipher system is thus improved.

3. Synchronization Error

In this section, we will show that the time-varying impulsive intervals do not effect the synchronization of two identical chaotic circuits embedded in the cipher transmitter and the cipher receiver. And it is possible to estimate the time required for synchronization.

Based on (1) and (4), let $e^T = (e_x, e_y, e_z) = (x_1 - \tilde{x}_1, x_2 - \tilde{x}_2, x_3 - \tilde{x}_3)$ be the synchronization error and $\tilde{X} = (\tilde{x}_1, \tilde{x}_2, \tilde{x}_3)^T$. Then

$$\begin{cases} \dot{e} = Ae + \Psi(X, \tilde{X}); & t \neq \tau_n \quad n = 1,2,\cdots \\ e(\tau_n^+) = (I+B)e(\tau_n) + B[Q(X(\tau_n^+)) - X(\tau_n^+)], & n = 1,2,\cdots \end{cases} \tag{9}$$

where $\Psi(X, \tilde{X}) = [-\alpha k \cdot f(x_1) + \alpha k \cdot f(x_1), 0, 0]^T$.

The Lyapunov function $V(e)$ can be depicted as $V(e) = e^T e = \|e\|^2$. And $\dot{V}(e) \le (\nu + 2|\alpha a|)V(e)$ then

$$\begin{aligned} V(e(\tau_n^+)) &\le d_1 V(e(\tau_n)) + \|B\|^2 \frac{q^2}{4} + q\|B\| d_1^{0.5} \|e(\tau_n)\| \\ &\le d_1 V(e(\tau_n)) + c_1 q \end{aligned} \tag{10}$$

Where $q = 2[Q(X(\tau_n^+)) - X(\tau_n^+)]$, and $c_1 = \|B\|^2 q/4 + \|B\| d_1^{0.5} \sup(\|e(\tau_n)\|)$. Since $\|e(\tau_n)\|$ is always bounded [7], and c_1 is a finite number also.

It is easy to denote $\lambda(\tau) = (\nu + 2|\alpha a|)\tau$ for $\dot{V}(e)$ and let

$$\begin{aligned} \overline{w} = d_1 c_1 (&\exp((\nu + 2|\alpha a|)(\Delta_1 + \Delta_2)) \\ &+ \exp((\nu + 2|\alpha a|)\max\{\Delta_1, \Delta_2\})) \end{aligned}$$

Based on the equation of (10), it is easy to expand as

$$\begin{aligned} &V(e(\tau_{2n}, t_0, e_0)) \\ &\le V(e(\tau_{2n-1}^+, t_0, e_0))\exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1})) \\ &\le (\mathrm{d}_1 V(e(\tau_{2n-1}, t_0, e_0)) + c_1 q)\exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1})) \\ &\le (\mathrm{d}_1 V(e(\tau_{2n-2}, t_0, e_0)) + c_1 q) \\ &\quad \times e\exp(\lambda(\tau_{2n-1}) - \lambda(\tau_{2n-2})) + c_1 q) \\ &\quad \times \exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1})) \\ &\quad = \mathrm{d}_1^2 \exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-2}))V(e(\tau_{2n-2}, t_0, e_0)) \\ &\qquad + \mathrm{d}_1 \mathrm{c}_1 \exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1}))q \\ &\qquad + \mathrm{d}_1 \mathrm{c}_1 \exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-2}))q \end{aligned} \tag{11}$$

From equation of (7), the $d_1^2 \exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-2})) \le (1/\xi^2)$. Thus

$$\begin{aligned} V(e(\tau_{2n}, t_0, e_0)) &\le \frac{1}{\xi^2} Ve(\tau_{2n-2}, t_0, e_0)) + \overline{w}q \\ &\le \frac{V(e_0)}{\xi^{2n}} + \frac{\xi^2 \overline{w}}{\xi^2 - 1} q. \end{aligned} \tag{12}$$

So, for any $\tau_{2n} < t < \tau_{2n+1}$, and $n \ge 1$, we have

$$\begin{aligned} V(e(t, t_0, e_0)) &\le V(e(\tau_{2n}^+, t_0, e_0))\exp(\lambda(t) - \lambda(\tau_{2n})) \\ &\le (\mathrm{d}_1 V(e(\tau_{2n}, t_0, e_0)) + c_1 q) \\ &\quad \times \exp(\lambda(t) - \lambda(\tau_{2n})) \\ &\le \left(\frac{d_1 V(e_0)}{\xi^{2n}} + \frac{d_1 \xi^2 \overline{w}}{\xi^2 - 1} q + c_1 q \right) \\ &\quad \times \exp((\nu + 2|\alpha a|)\max\{\Delta_1, \Delta_2\}) \end{aligned} \tag{13}$$

At the situation of $\left| K\|X\| - K\|\tilde{X}\| \right| < 1$. Where $\left| \|X\| - \|\tilde{X}\| \right|^2 \le V(e(t, t_0, e_0))$. Therefore the synchronous error can be minimized and

$$\begin{aligned} n \ge \log_{\xi^2} (&d_1 V(e_0) \cdot ((K^2 \exp((\nu + 2|\alpha a|) \\ &\times \max\{\Delta_1, \Delta_2\}))^{-1} - c_1 q - \frac{d_1 \xi^2 \overline{w}}{\xi^2 - 1} q)^{-1} \end{aligned} \tag{14}$$

Then the limited synchronization time is easy to estimate as the maximum synchronous error times the pre-defined frame interval, i.e.

$$t_{syn} = n \cdot (T_{2i-1} + T_{2i}) \tag{15}$$

where T_{2i-1} and T_{2i} are pre-defined frame interval.

After t_{syn}, the chaotic system in receiver will be synchronized with the transmitter. Based on the equation (14) and (15), the value of K will influence the synchronization time of two identical chaotic systems and the desired precision. Enlarge the K value will require a longer synchronization time. On the other hand, the security of the system is higher with a larger K and the sin nonlinear term (sin term will affect the $V(e)$). A tradeoff should be obtained in practice consideration.

4. Experimental Results

In this section, some experimental results illustrate the results of the proposed new nonlinear chaotic secure communication system. In this study, we select the parameter as $k = 1$, $\alpha = 9.35$, $\beta = 14.79$, $\gamma = 0.02$,

$a=-1.14$ and $b=-0.72$ to be initiated. Set $\nu=14.41$, choose the impulsive controller $\varepsilon_1=0.5$, and matrix B as

$$B=\begin{bmatrix}-1.05 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{bmatrix}$$

and $d_1=0.0024$. For any ξ satisfying $\xi>1$ and $0<|\xi d_1|\le 1$, we choose $\xi=310$. In order to synchronize the two chaotic systems of same parameters in (1) and (4), the transceiver has to satisfy Δ_1 which is derived from equation (7), that is

$$\Delta_1 \le \frac{-2(\ln(\xi)+2\ln|\theta+1|)}{1.5(\nu+2|a\alpha|)} \approx 10.6ms$$

Choose the frame length as $T_{2i-1}=5ms$ and $T_{2i}=2ms$. The initial condition is given by $[x_1(0),\ x_2(0),\ x_3(0)]=[-2.12;\ -0.05;\ 0.8]$; $[\tilde{x}_1(0),\ \tilde{x}_2(0),\ \tilde{x}_3(0)]=[-0.2;\ -0.02;\ 0.1]$, respectively. So the cipher and decipher are initially not synchronized, and the initial error is $e(0)=[-1.92;\ -0.03;\ 0.7]$. We choose the magnifying issue as $K=1000$ and $\lambda=12$. The quantization step is $q=5\times10^{-8}$. Numerical calculating the required synchronization time, let $n\ge 6$, and $t_{syn}=n\cdot(T_{2i-1}+T_{2i})=42ms$. Therefore, the cryptosystem will be synchronized in a 42ms process by impulsive control. The synchronization time is almost the same with the original Chua's chaotic system. After the cipher and decipher are synchronized, they will generate the same key sequences.

Use the tool of MathCAD to solve the partial differential matrix equations. And plot the chaotic results, using the mean and variance to identify the results. Table 1 shows the available parameter range of non-piecewise linear chaotic system, which is useful to many applications.

Tab. 1. Available parameter range of non-piecewise linear chaotic system

parameter	available chaotic range
α	8.82 ~ 10.91
β	12.19 ~ 16.10
γ	-0.24 ~ 0.11
a	-9 ~ -1.08
b	-0.88 ~ -0.33

Consider the 8bits embedded CPU efficient workable area; the limitation of 256 (-123 ~ +122) is good for applications. Then the a parameter available range will be sited on -9 to -1.08. That is, the smallest value of the parameter a will be approached to -9.

The other results are depicted as bellow: Fig. 1. to Fig. 3, the result of α=10.91, x(t), y(t), and z(t) phase relations. Fig. 4 as α=10.91, x(t), y(t), z(t) time domain relations. Fig. 5 to Fig. 7, let α=10.92, x(t), y(t), and z(t) phase relations. The value of α out of the available range, so it can not illustrate out the chaotic phenomenon. Fig. 8, time domain results of parameter α=10.92, x(t), y(t), and z(t), clearly, it can not worked on the chaotic situation for α=10.92. Fig. 9, the parameter β=12.19, x(t) and y(t) phase relationship, Fig. 10, the parameter of β=12.19, time domain result. Fig. 11, γ= -0.11, x(t) and y(t) phase relations. Fig 12, γ= -0.11, x(t), y(t), and z(t) time domain result. Fig. 13, a= -1.08, x(t) and y(t) phase relations. Fig. 14, a= -1.08, x(t), y(t), and z(t) time domain result. Fig. 15, b= -0.88, x(t) and y(t) phase relations. Fig. 16, b= -0.88, x(t), y(t), and z(t) time domain result. All parameters depict the proposed formula are all fit on nonlinear phenomenon.

5. Conclusions

This paper presented a new digital non-piecewise linear Chua's chaotic communication system by introducing a nonlinear –sin(x) term to randomize the nonlinear observed errors. Synchronization error and maximum t_{syn} time are derived out theoretically. This proposed nonlinear system is spread wider than the conventional Chua's cryptographic scheme and easy for 8 bits CPU implementation. Spread wider means for intruder there are more nonlinear items to be guessed. The available

chaotic ranges are fully listed for all parameters at table 1. This secure system is shown to be able to approach the one time pad scheme.

References

[1] T. Kapitaniak, ***Chaos for Engineers : Theory, Applications, and Control***, 2th ed., U.S.A: Springer, 2000.

[2] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with application to communication," ***IEEE Trans. Circuits Syst. I***, Vol. 40, No. 10, pp. 626–633, 1993.

[3] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," ***IEEE Trans. Circuits Syst. I,*** Vol. 44, No. 5, pp. 469–472, 1997.

[4] H. Zhou and Y. T. Ling, "Problems with the chaotic inverse system encryption approach," ***IEEE Trans. Circuits Syst. I,*** Vol. 44, No. 3, pp. 268–271, 1997.

[5] Z. G. Li, C. Y. Wen, and Y. C. Soh, "Analysis and design of impulsive control systems," ***IEEE Trans. Automat. Contr.,*** Vol. 46, No. 6, pp. 894–897, 2001.

[6] Z. G. Li, C. Y. Wen, Y. C. Soh, and W. X. Xie, "The stabilization and synchronization of Chua's oscillators via impulsive control," ***IEEE Trans. Circuits Syst. I,*** Vol. 48, No. 11, pp. 1351–1355, 2001.

[7] T. Yang and L. O. Chua, "Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication," ***IEEE Trans. Circuits Syst. I,*** Vol. 44, No. 10, pp. 976–988, 1997.

[8] K. Li, Y. C. Soh, and Z. G. Li, "Chaotic cryptosystem with high sensitivity to parameter mismatch," ***IEEE Trans. Circuits Syst. I,*** Vol. 50, No. 4, pp. 579–583, 2003.

[9] K. Li, Y. C. Soh, C. Y. Wen and Z. G. Li, "A new chaotic secure communication system," ***IEEE Trans. Commun***., Vol. 51, No. 8, pp. 1306–1312, 2003.

[10] J. Cruz and L. O. Chua, "An IC chip of Chua's circuit," ***IEEE Trans Circuits Syst. I,*** Vol. 40, No. 10, pp. 614–625, 1993.

[11] G. Heidari-Bsteni and C. MCGillem, "A chaotic direct-sequence spreadspectrum communication system," ***IEEE Trans. Commun.,*** Vol. 42, No. 2/3/4, pp. 1524–1527, 1994.

[12] L. O. Chua, "Chua's circuit—An overview ten years later," ***J. Circuit, Syst., Comput.,*** Vol. 4, No. 2, pp. 117–159, 1994.

[13] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic system with applications to secure communication systems," ***Int. J. Bifurc. Chaos,*** Vol. 3, No. 6, pp. 1619–1627, 1993.

[14] L. O. Chua, M. Itoh, L. Kocarev, and K. Eckert, "Chaos synchronization in Chua's circuit," ***J. Circuit Syst. Comput.***, Vol. 3, No. 1, pp. 93–108, 1993.

[15] K. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos," ***IEICE Trans. Commun.,*** Vol. 3, No. 2, pp. 469–477, 1993.

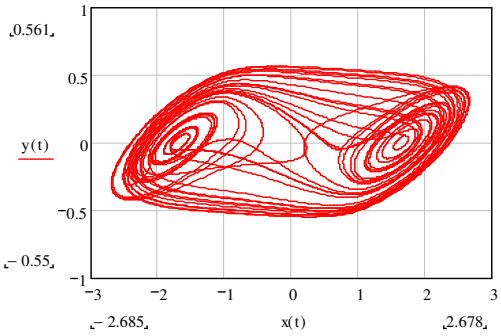

Fig. 1. α =10.91, x(t) and y(t) phase relationship

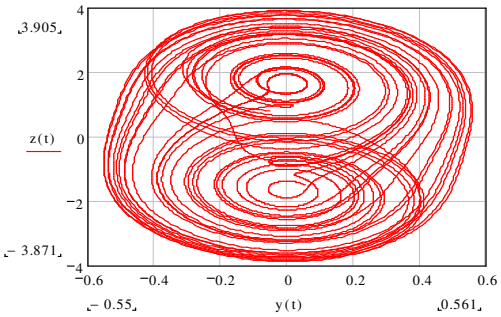

Fig. 2. α =10.91, y(t) and z(t) phase relationship

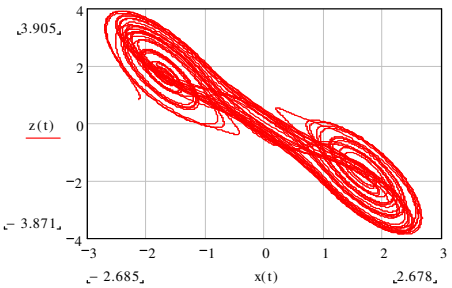

Fig. 3. α=10.91, x(t) and z(t) phase relationship

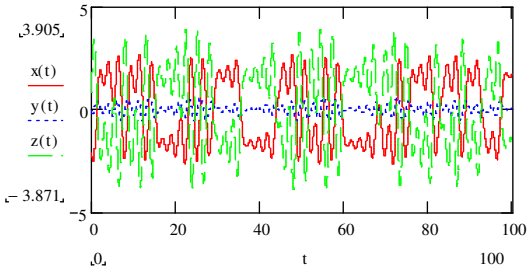

Fig. 4. α=10.91, x(t), y(t), and z(t) time domain result

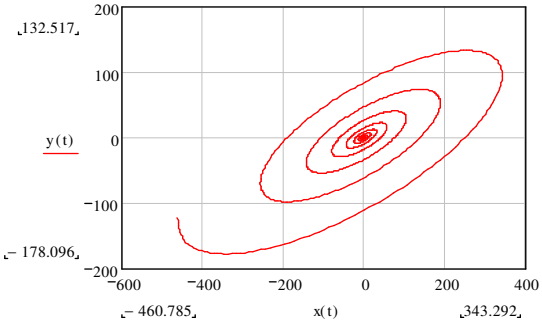

Fig. 5. α=10.92, x(t) and y(t) phase relationship

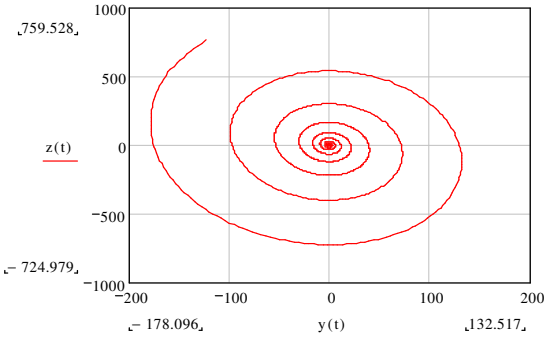

Fig. 6. α=10.92, y(t) and z(t) phase relationship

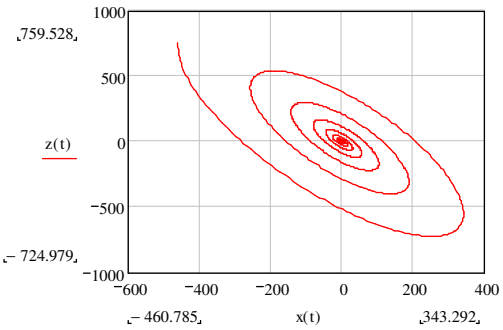

Fig. 7. α=10.92, x(t) and z(t) phase relationship

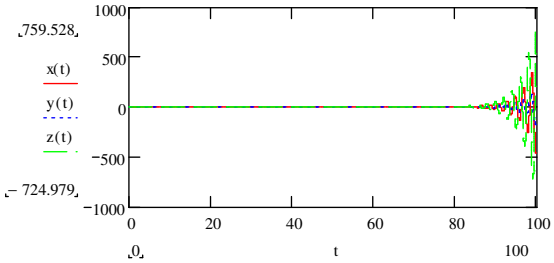

Fig. 8. α=10.92, x(t), y(t), and z(t) time domain result

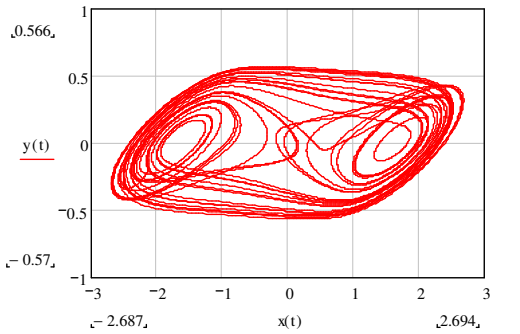

Fig. 9. β=12.19, x(t) and y(t) phase relationship

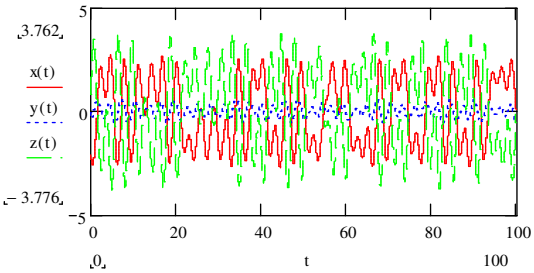

Fig. 10. β=12.19, x(t), y(t), and z(t) time domain result

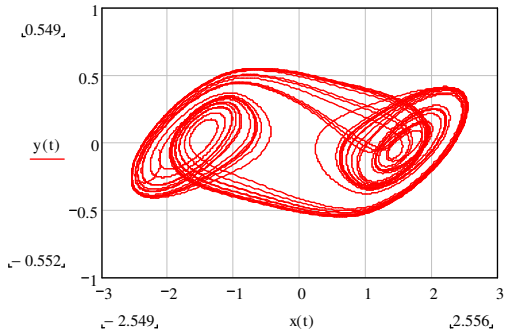

Fig. 11. γ **= -0.11, x(t) and y(t) phase relationship**

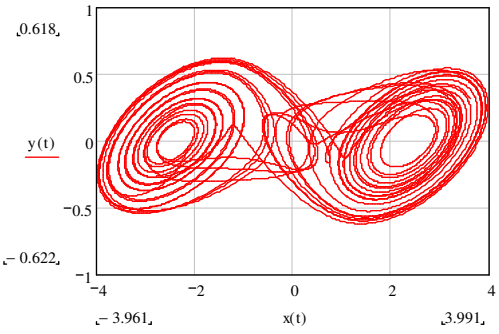

Fig. 15. b **= -0.88, x(t) and y(t) phase relationship**

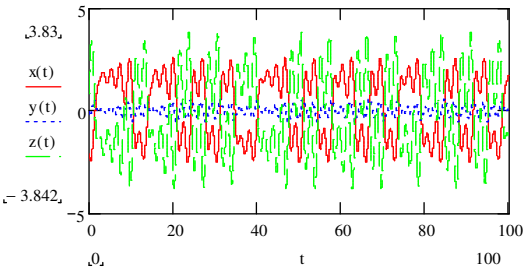

Fig. 12. γ **= -0.11, x(t), y(t), and z(t) time domain result**

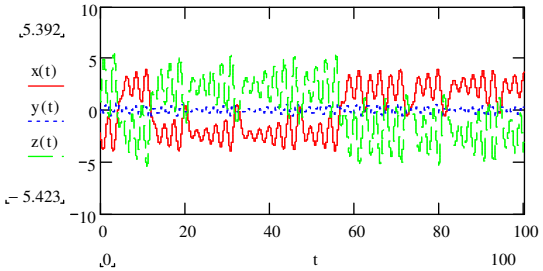

Fig. 16. b **= -0.88, x(t), y(t), and z(t) time domain result**

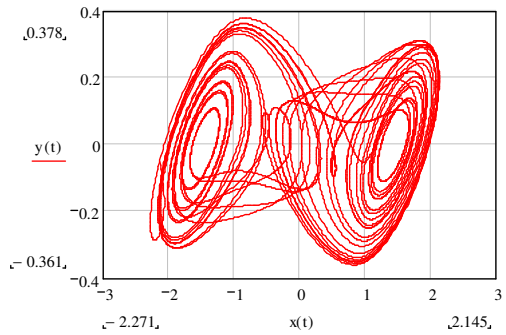

Fig. 13. a **= -1.08, x(t) and y(t) phase relationship**

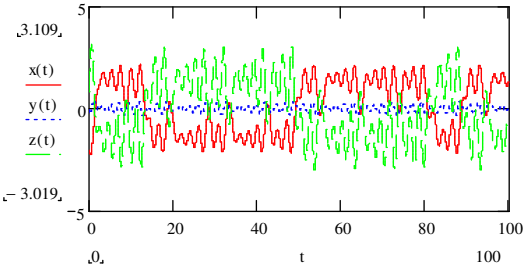

Fig. 14. a **= -1.08, x(t), y(t), and z(t) time domain result**