CRYPTOSYSTEMS BASED ON SYNCHRONIZED CHUA'S CIRCUITS [1]

César Cruz-Hernández [2]
and Hazael Serrano-Guerrero

Telematics Direction,
Scientific Research and Advanced Studies of Ensenada
(CICESE),
Km. 107, Tijuana-Ensenada, 22860 Ensenada, B. C.,
México.

Abstract: An experimental study of physical realization to encrypt private information using chaotic cryptosystems is presented. In particular, we use chaos synchronization and a complex encryption function to hide the messages. In both cryptosystems; encryption and synchronization are completely separated with no interference between them. We apply this approach to encrypt private analog and binary information signals. The utilization of chaos synchronization and cryptography seems to make a contribution to the development of communication systems with higher security.

Keywords: Chaos synchronization, Chua's circuit, observers, secure communication, encryption, experimental realization.

1. INTRODUCTION

Chaos synchronization has attracted much attention in recent years. This property is supposed to have interesting applications in different fields, particularly to design secure communication systems. A lot of chaos synchronization methods are being currently proposed in the literature, see e.g. (Pecora and Carroll, 1990; Nijmeijer and Mareels, 1997; Special Issue, 1997; 2000; Cruz-Hernández and Nijmeijer, 2000; Sira-Ramírez and Cruz-Hernández, 2001, and references therein).

Data encryption based on chaos synchronization was reported in the early 1990s (Pecora and Carroll, 1990), as a new approach for signal encoding which differs from the conventional methods using numerical algorithms as the encryption key. The issue of security, however, naturally arises in chaotic encryption, and it constitutes an important motivation for chaotic communication research. Whereby, several techniques, such as *chaotic additive masking*, *chaotic switching*, and *chaotic parameter modulation* have been developed. However, subsequent works, see e.g. (Short, 1994; Pérez and Cerdeira, 1995; Yang, 1995) have shown that encrypted signals by means of comparatively 'simple' chaos with only one positive Lyapunov exponent does not ensure a sufficient level of security. In some cases, extracting of information can be performed using common signal processing techniques, short-time zero-crossing rate, and return map based method.

Two factors of primordial importance in security considerations related to chaotic communication

[1] This work was supported by the CONACYT, México under Research Grant No. 31874-A.
[2] César Cruz-Hernández, CICESE, Telematics Direction., P.O. Box 434944, San Diego, CA 92143-4944, USA, Phone: +52.61.750500, Fax: +52.61.750537, E-mail: ccruz@cicese.mx

systems, are: the dimensionality of the chaotic attractor, and the effort required to obtain the necessary parameters for the matching of a receiver dynamics.

On the basis of these considerations, one way to enhance the level of security of the communication system can consist in applying proper *cryptographic techniques* to the private information signal (Yang, *et al.*, 1997). Another way to solve this security problem is to encode the message by using *high dimensional chaotic attractors*, or *hyperchaotic attractors*, which take advantage of the increased randomness and unpredictability of the higher dimensional dynamics. In such option, one generally encounters multiple positive Lyapunov exponents. However, hyperchaos synchronization is a much more difficult problem, see e.g. (Brucoli *et al.*, 1999; Cruz-Hernández *et al.*, 2002). The level of security is also enhanced by using chaos generators modeled by *delay differential equations*, such systems have an infinite-dimensional state space, and can produce hyperchaotic dynamics with an arbitrarily large number of positive Lyapunov exponents. This property claims to have low detectability, see e.g. (Mensour and Longtin, 1998; Pyragas, 1998; Cruz-Hernández, 2004).

The objective of this paper is to present the physical realization of two cryptosystems based on chaos synchronization and cryptography. The aim is to enhance the level of information security. In particular, we show that experimental synchronization of Chua's circuits is possible through a Generalized Hamiltonian forms and observer approach developed in (Sira-Ramírez and Cruz-Hernández, 2001).

2. CRYPTOSYSTEMS BASED ON SYNCHRONIZED CHUA'S CIRCUITS

In this section, we propose two cryptosystems based on synchronized Chua's circuits to encrypt analog and binary information signals. In both cryptosystems; encryption and synchronization are completely separated with no interference between them. The algorithm is composed of three steps: *encryption*, *synchronization*, and *decryption*. In each step, we try to retain the best features of existing schemes while avoiding their disadvantages. For example, like (Yang *et al.*, 1997), we use the same complex encryption function to hide the messages, but with the substantial difference that, we use a Generalized Hamiltonian forms and observer approach to synchronize chaotic generators developed in (Sira-Ramírez and Cruz-Hernández, 2001). As explained in (Yang *et al.*, 1997), using 'more' chaotic states other than the single transmitted signal in the encryption

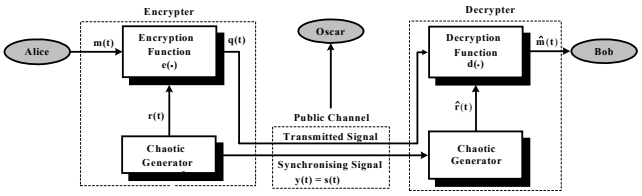


Fig. 1. Encrypter with two communication channels.

step increases the technical difficulty to recover the chaotic states, and thereby enhances security/privacy.

2.1 Cryptosystem: two communication channels

Figure 1 shows a block diagram of chaotic cryptosystem with two communication channels. $m(t)$ denotes the plain text signal (message), and $\hat{m}(t)$ the recovered message. The **encrypter** consists of a chaotic generator, and an encryption function $e(\cdot)$. The key signal $r(t)$ is one state of the chaotic generator and is used to encrypt the plain signal. $q(t)$ is the encrypted signal, which is sent to the decrypter via other communication channel. The signal $y(t) = s(t)$ is another state of the chaotic generator, which is transmitted through a public channel to the decrypter, and used to synchronize the chaotic generators.

The **decrypter** consists of a chaotic generator and a decryption function $d(\cdot)$. The chaotic generator is built to synchronize with the chaotic generator (of the encrypter), and can find the key signal $\hat{r}(t)$ when the chaotic generators are synchronized. $d(\cdot)$ is used to decrypt $\hat{m}(t)$ from $\hat{r}(t)$ and $q(t)$.

The **encrypted signal** $q(t)$ is obtained as

$$q(t) = e(m(t)). \tag{1}$$

The **encryption function** $e(\cdot)$ is defined by

$$\begin{aligned} e(m(t)) &= \underbrace{f_1(\cdots f_1(f_1}_{n\ times}(m(t), \underbrace{r(t)), r(t)), \cdots, r(t))}_{n\ times} \\ &= q(t) \end{aligned}$$

where $f_1(\cdot,\cdot)$ is the following nonlinear function

$$f_1(m,r) = \begin{cases} (m+r) + 2h, & -2h \le (m+r) \le -h, \\ (m+r), & -h < (m+r) < -h, \\ (m+r) - 2h, & h \le (m+r) \le 2h \end{cases}$$

with h chosen such that $m(t)$ and $r(t)$ lie within $(-h, h)$.

The **decryption function** $d(\cdot)$ is defined by

$$\begin{aligned} d(q(t)) &= e(q(t)) \\ &= \underbrace{f_1(\cdots f_1(f_1}_{n\ times}(q(t), \underbrace{-\hat{r}(t)), -\hat{r}(t)), \cdots, -\hat{r}(t))}_{n\ times} \\ &= \hat{m}(t). \end{aligned}$$

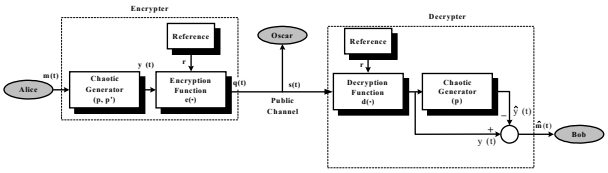


Fig. 2. Encrypter with one communication channel.

Remark 1. Note that $s(t) \neq q(t)$, i.e., the processes of encryption and synchronization are not mixed. So, encrypted signal doesn't interfere with synchronization, therefore not increasing the sensitivity of synchronization to external errors. As a result, the chaotic cryptosystem with two communication channels gives faster synchronization and higher security/privacy.

2.2 Cryptosystem: one communication channel

As second communication scheme, we propose the binary cryptosystem using a single communication channel (see Fig. 2), this objective is achieved by chaotic switching technique. Here, the binary message $m(t)$ is used to modulate one or more parameters of the (switching) encrypter, i.e. $m(t)$ controls a switch whose action changes the parameter values of the encrypter. Thus, according to the value of $m(t)$ at any given time t, the chaotic generator has either the parameter set value p or the parameter set p'. At the decrypter $m(t)$ is decoded by using the synchronization error ($e_y(t) = y(t) - \hat{y}(t) = \hat{m}(t)$) to decide whether signal corresponds to one parameter value, or the other (it can be interpreted as an "1" or "0"), i.e. synchronization or no synchronization between the chaotic generators. A particular state of the chaotic generator ($y(t)$) and a constant reference signal r are used by the encryption function $e(\cdot)$ to encrypt the plain signal $m(t)$. $q(t) = s(t)$ is the encrypted signal which is sent to the decrypter through a public channel. The inputs to decryption function $d(\cdot)$ are $q(t) = s(t)$, and the constant reference signal $-r$ to recover the chaotic sincronising signal $y(t)$ between the chaotic generators. So, the original message $m(t)$ is recovered by synchronization error detection ($e_y(t) = 0$, or $e_y(t) \neq 0$). The **transmitted and encrypted signal** $s(t)$ is obtained by

$$s(t) = q(t) = e(y(t)), \tag{2}$$

where the **encryption function** $e(\cdot)$ is

$$e(y(t)) = \underbrace{f_1(\cdots f_1(f_1}_{n\ times}(y(t), \underbrace{r), r), \cdots, r)}_{n\ times} = q(t).$$

The **decryption function** $d(\cdot)$ is defined by

$$\begin{aligned} y(t) &= d(q(t)) = e(q(t)) \\ &= \underbrace{f_1(\cdots f_1(f_1}_{n\ times}(q(t), \underbrace{-r), -r), \cdots, -r)}_{n\ times}. \end{aligned}$$

In this work, we use the Chua's circuit as chaotic generator for both cryptosystems. In particular, in *cryptosystem with two communication channels*: $s(t) = y(t) = x_1(t)$ is the sincronising signal for chaotic generators, and $r(t) = x_2(t)$ is the key signal used to encrypt the plain text $m(t)$. Finally, $\hat{r}(t) = \xi_2(t)$ is the recovered key signal obtained from the Chua's circuit of decrypter. In *cryptosystem with one communication channel*: $y(t) = x_1(t)$, $\hat{y}(t) = \xi_1(t)$, $q(t) = s(t)$. In next section, we will establish the particular equations for chaotic generator of encrypter (Chua's circuit in Generalized Hamiltonian form), and for chaotic generator of decrypter (state observer of Chua's circuit). Thus, we will obtain the synchronization between them.

3. SYNCHRONIZATION OF CHUA'S CIRCUIT

Consider the following dynamical system

$$\dot{x}(t) = f(x(t)), \qquad x \in \mathbb{R}^n \tag{3}$$

which represents an oscillator exhibiting a **chaotic** behavior. Following the approach provided in (Sira-Ramírez and Cruz-Hernández, 2001), many physical systems described by Eq. (3) can be written in the following "*Generalized Hamiltonian" canonical* form,

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + \mathcal{S}(x)\frac{\partial H}{\partial x} + \mathcal{F}(x), \tag{4}$$

$H(x)$ denotes a smooth *energy function* which is globally positive definite in $\mathbb{R}^n$. The *gradient* of H, denoted by $\partial H/\partial x$, is assumed to exist everywhere. We use quadratic energy function $H(x) = 1/2\, x^T \mathcal{M} x$ with $\mathcal{M} = \mathcal{M}^T > 0$. In such case, $\partial H/\partial x = \mathcal{M} x$. The matrices $\mathcal{J}(x)$ and $\mathcal{S}(x)$ satisfy, for all $x \in \mathbb{R}^n$, the following properties, which clearly depict the *energy managing* structure of the system, $\mathcal{J}(x) + \mathcal{J}^T(x) = 0$ and $\mathcal{S}(x) = \mathcal{S}^T(x)$. The vector field $\mathcal{J}(x)\,\partial H/\partial x$ exhibits the *conservative* part of the system and it is also referred to as the *workless* part, or *workless* forces of the system; and $\mathcal{S}(x)$ depicting the *working* or *nonconservative* part of the system. For certain systems, $\mathcal{S}(x)$ is *negative definite* or *negative semidefinite*. In such cases, the vector field is addressed to as the *dissipative* part of the system. If, on the other hand, $\mathcal{S}(x)$ is positive definite, positive semidefinite, or indefinite, it clearly represents, respectively, the global, semi-global, and local *destabilizing* part of the system. In the last case, we can always (although nonuniquely) decompose such an indefinite symmetric matrix

into the sum of a symmetric negative semidefinite matrix $\mathcal{R}(x)$ and a symmetric positive semidefinite matrix $\mathcal{N}(x)$. $\mathcal{F}(x)$ represents a *locally destabilizing* vector field.

For **synchronization** purposes, we consider a special class of Generalized Hamiltonian forms with destabilizing vector field and linear output map, $y(t)$, **(chaotic generator/encrypter for both cryptosystems)** given by

$$\begin{aligned} \dot{x} &= \mathcal{J}(y)\frac{\partial H}{\partial x} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial x} + \mathcal{F}(y), \qquad x \in \mathbb{R}^n \\ y &= \mathcal{C}\frac{\partial H}{\partial x}, \qquad y \in \mathbb{R}^m \end{aligned} \tag{5}$$

$\mathcal{S}$ is a constant symmetric matrix, not necessarily of definite sign. $\mathcal{I}$ is a constant skew symmetric matrix. $\mathcal{C}$ is a constant matrix.

We denote the *estimate* of the state $x(t)$ by $\xi(t)$, and consider the Hamiltonian energy function $H(\xi)$ to be the particularization of H in terms of $\xi(t)$. Similarly, we denote by $\eta(t)$ the estimated output, computed in terms of $\xi(t)$. The gradient $\partial H(\xi)/\partial\xi$ is, naturally, of the form $\mathcal{M}\xi$ with $\mathcal{M} = \mathcal{M}^T > 0$.

A dynamic *nonlinear state observer* for the system (5) **(chaotic generator/decrypter for both cryptosystems)** is obtained as

$$\begin{aligned} \dot{\xi} &= \mathcal{J}(y)\frac{\partial H}{\partial \xi} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial \xi} + \mathcal{F}(y) + K(y-\eta), \\ \eta &= \mathcal{C}\frac{\partial H}{\partial \xi} \end{aligned} \tag{6}$$

K is known as the *observer gain.*

The *state estimation error*, defined as $e(t) = x(t) - \xi(t)$ and the output estimation error, defined as $e_y(t) = y(t) - \eta(t)$, are governed by

$$\begin{aligned} \dot{e} &= \mathcal{J}(y)\frac{\partial H}{\partial e} + (\mathcal{I}+\mathcal{S}-K\mathcal{C})\frac{\partial H}{\partial e}, \; e \in \mathbb{R}^n \\ e_y &= \mathcal{C}\frac{\partial H}{\partial e}, \quad e_y \in \mathbb{R}^m \end{aligned} \tag{7}$$

where $\partial H/\partial e$ actually stands, with some abuse of notation, for the gradient of the *modified* energy function, $\partial H(e)/\partial e = \partial H/\partial x - \partial H/\partial \xi = \mathcal{M}(x-\xi) = \mathcal{M}e$.

Chaotic synchronization problem: *We say that the chaotic generator/decrypter (6) synchronizes with the chaotic generator/encrypter (5), if*

$$\lim_{t\to\infty} \|x(t) - \xi(t)\| = 0, \tag{8}$$

no matter which initial conditions $x(0)$ and $\xi(0)$ have. $e(t) = x(t) - \xi(t)$ represents the synchronization error.

Chaotic generator (Chua's circuit): Consider the normalized form of the ordinary differential equations *(ODE) equivalents* of Chua's circuit (Pospísil *et al.*, 2000):

$$\begin{aligned} \dot{x}_1 &= -\alpha(b+1)x_1 + \alpha x_2 + \alpha(b-a)h(x_1), \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2, \end{aligned} \tag{9}$$

where the nonlinear function is given by

$$h(x_1) = \frac{1}{2}(|1+x_1| - |1-x_1|). \tag{10}$$

Chua's circuit (9)-(10) in Generalized Hamiltonian Canonical form (5), with a destabilizing vector field (as **chaotic generator/encrypter for both cryptosystems**) is given by

$$\begin{aligned} \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} \\ &+ \begin{bmatrix} -\alpha^2(b+1) & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x} \\ &+ \begin{bmatrix} \alpha(b-a)h(x_1) \\ 0 \\ 0 \end{bmatrix}, \end{aligned} \tag{11}$$

taking as Hamiltonian energy function

$$H(x) = \frac{1}{2}\left(\frac{1}{\alpha}x_1^2 + x_2^2 + \frac{1}{\beta}x_3^2\right). \tag{12}$$

The destabilizing vector field calls for $x_1(t)$ to be used as the output, $y(t)$ of the chaotic generator/encrypter (11). $\mathcal{C}$, $\mathcal{S}$, and $\mathcal{I}$ are given by

$$\mathcal{C} = \begin{bmatrix} \alpha & 0 & 0 \end{bmatrix}, \qquad \mathcal{S} = \begin{bmatrix} -\alpha^2(b+1) & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\mathcal{I} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix}.$$

The observer (as **chaotic generator/decrypter for both cryptosystems**) for dynamics (11) is designed as

$$\begin{aligned} \begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} \\ &+ \begin{bmatrix} -\alpha^2(b+1) & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} \\ &+ \begin{bmatrix} -\frac{1}{C_1}F(y) \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_1. \end{aligned} \tag{13}$$

From chaotic generator/encrypter (11) and chaotic generator/decrypter (13), the synchronization error dynamics is governed by

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \tag{14}$$

$$\begin{bmatrix} 0 & \frac{\alpha}{2}k_2 & \frac{\alpha}{2}k_3 \\ -\frac{\alpha}{2}k_2 & 0 & \beta \\ -\frac{\alpha}{2}k_3 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial e} +$$

$$\begin{bmatrix} -\alpha^2(b+1)-\alpha k_1 & \alpha(1-\frac{1}{2}k_2) & -\frac{\alpha}{2}k_3 \\ \alpha(1-\frac{1}{2}k_2) & -1 & 0 \\ -\frac{\alpha}{2}k_3 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial e}.$$

4. SYNCHRONIZATION STABILITY ANALYSIS

Now, we give conditions for stability of the synchronization error (14) between Chua's circuit in Hamiltonian canonical form (11) and state observer (13). A necessary and sufficient condition for global asymptotic stability to zero of the estimation error (14) is given by the following theorem.

Theorem 1. (Sira-Ramírez and Cruz-Hdez, 2001). The state $x(t)$ of system (11) can be globally, exponentially, asymptotically estimated, by the state $\xi(t)$ of the observer (13) if and only if there exists a constant matrix K such that the symmetric matrix

$$[\mathcal{I}+\mathcal{S}-K\mathcal{C}]+[\mathcal{I}+\mathcal{S}-K\mathcal{C}]^T=[\mathcal{S}-K\mathcal{C}]+[\mathcal{S}-K\mathcal{C}]^T$$
$$=2\left[\mathcal{S}-\frac{1}{2}\left(K\mathcal{C}+\mathcal{C}^TK^T\right)\right]$$

is negative definite.

In particular, for Chua's circuit $-\frac{1}{2}[K\mathcal{C}-K^T\mathcal{C}^T]$ is given by

$$\begin{bmatrix} -\alpha^2(b+1)-\alpha k_1 & \alpha(1-\frac{1}{2}k_2) & -\frac{\alpha}{2}k_3 \\ \alpha(1-\frac{1}{2}k_2) & -1 & 0 \\ -\frac{\alpha}{2}k_3 & 0 & 0 \end{bmatrix}$$

which is negative definite, if we choose k_1, k_2, and k_3 such that

$$\begin{aligned} k_1 &\leq -3.2, \\ 2.5k_2^2-10k_2+6.8 &\leq k_1, \\ k_3 &= 0. \end{aligned} \tag{15}$$

5. EXPERIMENTAL RESULTS

We present experimental results to illustrate our cryptosystems with two communication channels, and a single communication channel. The physical realization of encrypter and decrypter based on the normalized ODE equivalents of Chua's circuit (9)-(10) can carry out by using commercial electronic components, the details will appear in other place. In the following experiments, the choice of values: $\alpha = 20$, $\beta = 15.6$, $a = -1.27$, $b = -0.68$, $k_1 = 10$, $k_2 = 4$, $k_3 = 0$, $h = 10$, and $n = 10$ was used.

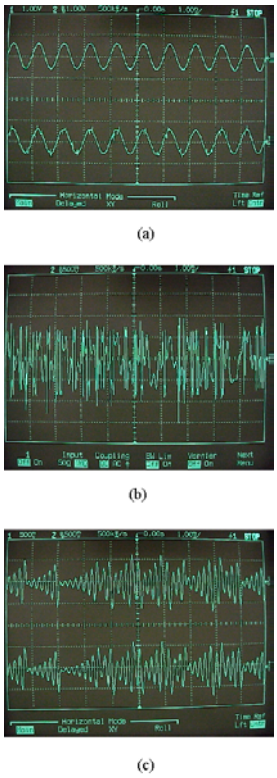


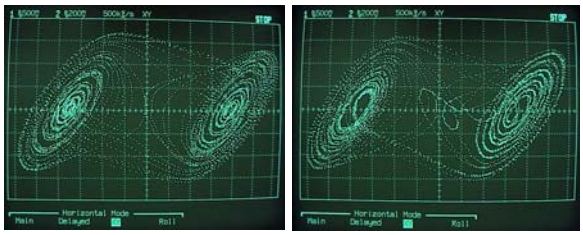
Fig. 3. Encryption with two communication channels: (a) $m(t)$: original message (top of figure), and $\hat{m}(t)$: recovered message (bottom of figure). (b) $q(t)$: encrypted signal. (c) Key signal $r(t) = x_2(t)$ (top of fugure), and recovered key signal $\hat{r}(t) = \xi_2(t)$ (bottom of figure).

5.1 Cryptosystem: two communication channels

Figure 3 shows the experimental results from circuit of the encrypter with two communication channels: the original message $m(t)$ (top of Fig. 3(a)), and the recovered message $\hat{m}(t)$ (bottom of Fig. 3(a)). The encrypted signal $q(t)$ (middle of figure). The key signal $r(t) = x_2(t)$ (top of Fig. 3(c)), and recovered key signal $\hat{r}(t) = \xi_2(t)$ (bottom of Fig. 3(c)).

5.2 Cryptosystem: one communication channel

We use a 'modulation rule' to encrypt and to transmit the binary message $m(t) = 0, 1$ as follows (α was fixed at encrypter and decrypter): at



(a) (b)

Fig. 4. (a) The chaotic attractor of Chua's circuit for encoding "0". (b) The chaotic attractor of Chua's circuit for encoding "1".

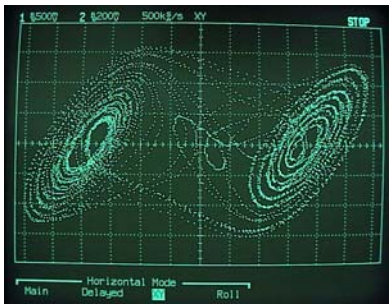


Fig. 5. The chaotic attractor of Chua's circuit (13) for detection of"1" at the decrypter.

encrypter, $\beta(t) = \beta + r \cdot m(t)$ with $r = 0.2$. β is switched between $\beta(0) = 15.6$ and $\beta(1) = 15.8$ to encode "0" and "1", respectively. The corresponding chaotic attractors of Chua's circuit are shown in Fig. 4: (a) illustrates the chaotic attractor of Chua's circuit (11) for encoding "0", $\beta(0) = 15.6$. (b) The chaotic attractor of Chua's circuit (11) for encoding "1", $\beta(1) = 15.8$. While Fig. 5 shows the chaotic attractor of Chua's circuit (13) with $\beta = 15.8$ for detection of "1"at decrypter.

6. CONCLUSIONS

We have proposed two cryptosystems which combine chaos synchronization with a nonlinear encryption function to encrypt confidential information, producing a more complex, and potentially, more encoder.

We have shown experimentally two chaotic cryptosystems using two communication channels, and a single communication channel to encrypt analog and binary information signals. In both cryptosystems, the algorithm is composed of three steps: encryption, synchronization, and decryption, with encryption and synchronization completely separated with no interference between them. As a result, the cryptosystems give faster synchronization and higher security.

The experimental results show very good (qualitative) agreement with the previous numerical results given in (Serrano-Guerrero and Cruz-Hernández, 2002).

7. REFERENCES

Brucoli, M., Cafagna, D. and Carnimeo L. (1999) Design of a hyperchaotic cryptosystem based on identical and generalized synchronization, *Int. J. Bifurc. Chaos* **9**(10), 2027-2037.

Cruz-Hernández, C. and Nijmeijer, H. (2000) Synchronization through extended Kalman filtering, *Int. J. Bifurc. Chaos* **10**(4), 763-775.

Cruz-Hernández, C., Posadas, C. and Sira-Ramírez, H. (2002) Synchronization of two hyperchaotic Chua circuits: A generalized Hamiltonian systems approach, *Procs. of the 15th IFAC World Congress*, Barcelona Spain.

Cruz-Hernández, C. (2004) Synchronization of time-delay Chua's oscillator with application to secure communication, *Nonlinear Dynamics and Systems Theory* **4**(1), 1-13.

Mensour, B. and Longtin, A. (1998) Synchronization of delay-differential equations with application to private communication, *Phys. Lett. A* **244**(1), 59-70.

Nijmeijer, H. and Mareels, I.M.Y. (1997) An observer looks at synchronization, *IEEE Trans. Circuits Syst. I* **44**(10) 882-890.

Pecora, L. M. and Carroll, T.L. (1990) Synchronization in chaotic systems,*Phys. Rev. Lett.* **64**, 821-824.

Pérez, G. and Cerdeira, H.A. (1995) *Phys. Rev. Lett.* **74** 1970-1973.

Pospísil, J., Kolka, Z., Horská, J. and Brzobohatý (2000) Simplest ODE equivalents of Chua's equations, *Int. J. Bifurc. Chaos* **10**(1), 1-23.

Pyragas, K. (1998) Transmission of signals via synchronization of chaotic time-delay systems, *Int. J. Bifurc. Chaos* **8**(9), 1839-1842.

Serrano-Guerrero, H. and Cruz-Hernández, C. (2002) Sistema encriptador con base en la sincronía de circuitos de Chua *Procs. of the 2th Conferencia Internacional Automática*, Santiago de Cuba, Cuba.

Short, K.M. (1994) Steps towards unmasking chaotic communication," *Int. J. Bifurc. Chaos* **4**(4) 959-977.

Sira-Ramírez, H. and Cruz-Hernández, C. (2001) Synchronization of chaotic systems: A Generalized Hamiltonian systems approach, *Int. J. Bifurc. Chaos* **11**(5), 1381-1395.

Special Issue (1997) on Chaos synchronization and control: Theory and applications, *IEEE Trans. Circuits Syst. I*, **44**(10).

Special Issue (2000) on Control and synchronization of chaos, *Int. J. Bifurc. Chaos*, **10**(34).

Yang, T. (1995) Recovery of digital signals from chaotic switching, *Int. J. Circuit Th. Appl.* **23**(6), 611-615.

Yang, T. , Wu, C.W. and Chua, L.O. (1997) Cryptography based on chaotic systems, *IEEE Trans. Circuits Syst. I* **44**(5), 469-472.