Communicating Confidential Information via Synchronized Time-Delay Chua's Circuits*

C. CRUZ-HERNANDEZ† and N. ROMERO-HAROS‡
Telematics Direction,
Scientific Research and Advanced Studies of Ensenada (CICESE),
Km. 107 Carretera Tijuana-Ensenada, 22860 Ensenada, B.C., México.

Abstract

In this work, we apply the Generalized Hamiltonian forms and observer approach to synchronize time-delay-feedback Chua's circuits to transmit confidential information. We show by means of two communication schemes the quality of the recovered information, and at the same time, we have enhance the level of encryption security.

Key-Words: Hyperchaos synchronization, time-delay Chua's circuit, observers, secure communication.

1 Introduction

Chaos synchronization has attracted much attention in recent years see e.g., [1-6]. This property is supposed to have interesting applications in different fields, particularly to design secure communication systems. Data encryption using chaotic dynamics was reported in the early 1990s as a new approach for encoding. Different techniques have been developed in order to hide information using chaos synchronization, such as *chaotic masking*, *chaotic switching*, and *chaotic parameter modulation*. However, it has been shown see e.g., [7] that encrypted signals by means of comparatively simple chaos with only one positive Lyapunov exponent does not ensure a sufficient level of security. For higher security the hyperchaotic systems characterized by more than one positive exponents are advantageous over simple chaotic systems. Two factors of primordial importance in security considerations related to chaotic communication 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 encryption security is by applying proper cryptographic techniques to the information [8, 9]. Another way is to encode information by using high dimensional chaotic attractors, or hyperchaotic attractors, which take advantage of the increased randomness and unpredictably of the higher dimensional dynamics. In such option, one generally encounters *multiple positive Lyapunov exponents*. However, the hyperchaos synchronization is a much more difficult problem (see e.g. [10-12] and [13] for discrete-time context). Most of the previous work done on hyperchaos synchronization has been concentrated on finite-dimensional systems described by ordinary differential equations. Thus, the number of positive Lyapunov exponents is limited by dimension of the state space.

As alternative way of constructing synchronized hyperchaotic systems can be based on delay differential equations, such systems have an infinite-dimensional state space and can produce hyperchaos with an arbitrarily large number of positive Lyapunov exponents. It has been known that even a very simple first-order oscillator with a time-delay can produce extremely complex hyperchaotic behaviors [14-15]. This property has stimulated the design of secure communication systems which claimed to have low detectability [16, 17].

The objective of this work is to use the Generalized Hamiltonian forms and observer approach developed in [5] to synchronize time-delay-feedback Chua's circuits. Moreover, we apply this approach to transmit confidential information. A similar idea was used in [18] with the substantial differences: the modified communication scheme used here, is such that the sent information can be recovered faithfully, and effects of noise in channel are considered.

2 Review of synchronization

Consider the dynamical system described by

$$\dot{x} = f\left(x,\, x\left(t-\tau\right)\right), \tag{1}$$

*This work was supported by the CONACYT, México under Research Grant No. 31874-A.

†**Correspondence to:** César Cruz-Hernández, CICESE, Telematics Direction, P.O. Box 434944, San Diego, CA 92143-4944, USA, Phone: +52.646.1750500, Fax: +52.646.1750537, E-mail: ccruz@cicese.mx

‡With Electronics and Telecom. Dept.

where $x(t) \in \mathbb{R}^n$ is the state vector, f is a nonlinear function, and τ is a time-delay. The system (1) provides an example of infinite-dimensional oscillator with *multiple positive Lyapunov exponents* (generating extremely complex hyperchaotic signals). Following the approach developed in [5], it was reported in [18] that the time-delay oscillator (1) can be written in *Generalized Hamiltonian canonical form*,

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + \mathcal{S}(x)\frac{\partial H}{\partial x} + \mathcal{F}(x, x(t-\tau)), \quad x \in \mathbb{R}^n, \tag{2}$$

$H(x)$ denotes a smooth *energy function* which is globally positive definite in $\mathbb{R}^n$. The *gradient vector* 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 $\mathcal{M}$ being a, constant, symmetric positive definite matrix. 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*. Thus, 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) descompose such an indefinite symmetric matrix into the sum of a symmetric negative semidefinite matrix $\mathcal{R}(x)$ and a symmetric positive semidefinite matrix $\mathcal{N}(x)$. Finally, $\mathcal{F}(x, x(t-\tau))$ represents a *locally destabilizing* vector field.

In the context of observer design, we consider a special class of Generalized Hamiltonian systems with destabilizing vector field and linear output map , $y(t)$, given by

$$\begin{aligned} \dot{x} &= \mathcal{J}(y)\frac{\partial H}{\partial x} + (\mathcal{I} + \mathcal{S})\frac{\partial H}{\partial x} + \mathcal{F}(y, y(t-\tau)), \;\; x \in \mathbb{R}^n \\ y &= \mathcal{C}\frac{\partial H}{\partial x}, \qquad y \in \mathbb{R}^m, \end{aligned} \tag{3}$$

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

We denote the *estimate* of the state vector $x(t)$ 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 the estimated state $\xi(t)$. The gradient vector $\partial H(\xi)/\partial \xi$ is, naturally, of the form $\mathcal{M}\xi$ with $\mathcal{M}$ being a, constant, symmetric positive definite matrix.

A *nonlinear state observer* for the Generalized Hamiltonian form (3) is given by

$$\begin{aligned} \dot{\xi} &= \mathcal{J}(y)\frac{\partial H}{\partial \xi} + (\mathcal{I} + \mathcal{S})\frac{\partial H}{\partial \xi} + \mathcal{F}(y, y(t-\tau)) + K(y - \eta), \\ \eta &= \mathcal{C}\frac{\partial H}{\partial \xi}, \end{aligned} \tag{4}$$

$\xi \in \mathbb{R}^n$ and K is 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

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

where the vector, $\partial H/\partial e$ actually stands, with some abuse of notation, for the gradient vector of the *modified* energy function, $\partial H(e)/\partial e = \partial H/\partial x - \partial H/\partial \xi = \mathcal{M}(x - \xi) = \mathcal{M}e$. We set, when needed, $\mathcal{I} + \mathcal{S} = \mathcal{W}$.

Remark 1 *Note that the error state dynamics described by Eq. (5) is independent of time-delay τ, i.e. Eq. (5) is a simple linear ordinary differential equation.*

Definition 1 ***Synchronization:*** *We say that the slave (4)* ***synchronizes*** *with the master (3), if*

$$\lim_{t \to \infty} \|x(t) - \xi(t)\| = 0, \tag{6}$$

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

3 Synchronization of time-delay-feedback Chua's circuit

Time-delay-feedback Chua's circuit considered in this work is shown in Figure 1, and can be described by [19]:

$$\begin{aligned} C_1\dot{x}_1 &= G(x_2 - x_1) - F(x_1), \\ C_2\dot{x}_2 &= G(x_1 - x_2) + x_3, \\ L\dot{x}_3 &= -x_2 - R_0 x_3 - w(x_1(t-\tau)), \end{aligned} \tag{7}$$

with $F(x_1)$ given by

$$F(x_1) = bx_1 + \frac{1}{2}(a-b)(|x_1+1| - |x_1-1|), \; a, b < 0, \tag{8}$$

and where the time-delay term is taken as

$$w(x_1(t-\tau)) = \varepsilon \sin(\sigma\, x_1(t-\tau)), \tag{9}$$

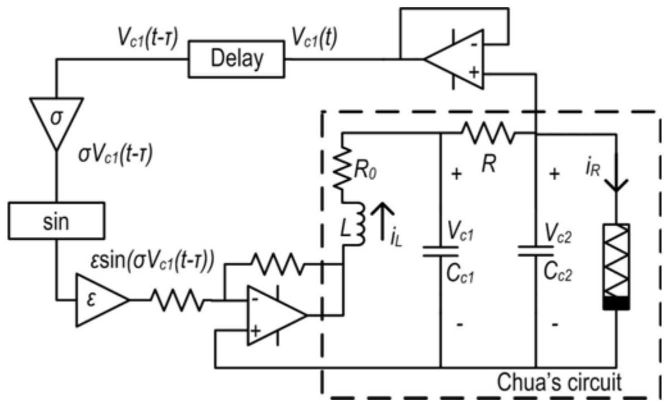

Figure 1: Time-delay-feedback Chua's circuit.

with ε and σ positive constants, and τ is a time-delay. The maximum amplitude of the time-delay term is

$$|w\left(x_1\left(t-\tau\right)\right)| \leq \varepsilon. \tag{10}$$

For arbitrarily given $\varepsilon > 0$, the time-delay-feedback Chua's circuit (7)-(8) can be hyperchaotic for sufficiently large σ and τ. To facilitate our discussion, we will resort to the *normalized version* of the time-delay feedback Chua's circuit [18]:

$$\begin{aligned} \dot{x}_1 &= \alpha\left(x_2 - x_1 - f\left(x_1\right)\right), \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 - \beta\,\varepsilon \sin\left(\sigma x_1\left(t-\tau\right)\right), \end{aligned} \tag{11}$$

with nonlinear function

$$f\left(x_1\right) = bx_1 + \frac{1}{2}\left(a-b\right)\left(|x_1+1| - |x_1-1|\right). \tag{12}$$

The time-delay-feedback Chua's circuit (11)-(12) in Hamiltonian canonical form (**master circuit**) is given by

$$\begin{aligned} \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} \\ &+ \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha f\left(x_1\right) \\ 0 \\ -\beta \sin\left(\sigma x_1\left(t-\tau\right)\right) \end{bmatrix} \end{aligned} \tag{13}$$

taking as the Hamiltonian energy function

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

and gradient vector as

$$\frac{\partial H}{\partial x} = \begin{bmatrix} \frac{1}{\alpha} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\beta} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \frac{1}{\alpha}x_1 \\ x_2 \\ \frac{1}{\beta}x_3 \end{bmatrix}.$$

The destabilizing vector field evidently calls for $x_1\left(t\right)$ to be used as the output, $y\left(t\right)$, of the master circuit (13). The matrices $\mathcal{C}$, $\mathcal{S}$, and $\mathcal{I}$, are given by

$$\mathcal{C} = \begin{bmatrix} \alpha & 0 & 0 \end{bmatrix}, \ \mathcal{S} = \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix}, \mathcal{I} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix}.$$

The pair $(\mathcal{C}, \mathcal{S})$ is neither observable nor detectable. However, the pair $(\mathcal{C}, \mathcal{W})$ is observable. The system lacks damping in the $x_3\left(t\right)$ state, and either in the $x_1\left(t\right)$ or the state $x_2\left(t\right)$ state as inferred from the negative semi-definite nature of the dissipation structure matrix, $\mathcal{S}$. If $x_1\left(t\right)$ is used as output, then the output error injection term can enhance the dissipation in the error state dynamics. The state observer for (13) (**slave circuit)** is designed as

$$\begin{aligned} \begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial \xi} \\ &+ \begin{bmatrix} -\alpha F\left(y\right) \\ 0 \\ -\beta \sin\left(\sigma y\left(t-\tau\right)\right) \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y, \end{aligned} \tag{14}$$

$K = \left(k_1, k_2, k_3\right)^T$ is chosen in order to guarantee the asymptotic exponential stability to zero of the state reconstruction error trajectories (synchronization error $e\left(t\right)$). From (13) and (14) the synchronization error dynamics is governed by

$$\begin{aligned} \begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} &= \begin{bmatrix} 0 & \frac{k_2\alpha}{2} & \frac{k_3\alpha}{2} \\ -\frac{k_2\alpha}{2} & 0 & 2\beta \\ -\frac{k_3\alpha}{2} & -2\beta & 0 \end{bmatrix} \frac{\partial H}{\partial e} \\ &+ \begin{bmatrix} -\alpha(\alpha + \frac{k_1}{2}) & \alpha\left(1 - \frac{k_2}{2}\right) & -\frac{k_3\alpha}{2} \\ \alpha\left(1 - \frac{k_2}{2}\right) & -1 & 0 \\ -\frac{k_3\alpha}{2} & 0 & -\sigma\beta \end{bmatrix} \frac{\partial H}{\partial e}. \end{aligned} \tag{15}$$

4 Stability of synchronization

We examine the stability of the synchronization error (15) between (13) and (14).

A necessary and sufficient condition for global asymptotic stability to zero of the estimation error is given by the following theorem.

Theorem 1 (5) *The state $x\left(t\right)$ of the nonlinear system (13) can be globally, exponentially, asymptotically estimated, by the state $\xi\left(t\right)$ of the observer (14) if and only if there exists a constant matrix K such that the symmetric matrix*

$$\begin{aligned} \left[\mathcal{W} - K\mathcal{C}\right] + \left[\mathcal{W} - K\mathcal{C}\right]^T &= \left[\mathcal{S} - K\mathcal{C}\right] + \left[\mathcal{S} - K\mathcal{C}\right]^T \\ &= 2\left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right] \end{aligned}$$

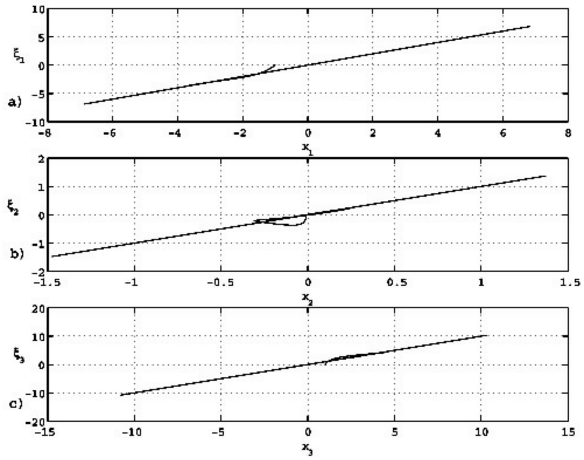

Figure 2: Synchronization between master (13) and slave (14) Chua's circuits.

is negative definite.

In particular, for time-delay-feedback Chua's circuit, $2\left[\mathcal{S}-\frac{1}{2}\left(K\mathcal{C}+\mathcal{C}^T K^T\right)\right]$ is given by

$$\left[\begin{array}{ccc} -2\left(\alpha^2+k_1\right) & 2\alpha-k_2 & -k_3 \\ 2\alpha-k_2 & -2 & 0 \\ -k_3 & 0 & -2\gamma\beta \end{array}\right]$$

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

$$\begin{aligned} k_1 &\geq 0\,, \\ k_2 &< 2\alpha+\left(\frac{1}{\gamma\beta}k_3^2+4k_1+4\alpha^2\right)^{\frac{1}{2}}, \\ k_3 &< 2\left(\gamma\beta\left(k_1+\alpha^2\right)\right)^{\frac{1}{2}}. \end{aligned} \tag{16}$$

Figure 2 shows the synchronization between master (13) and slave (14) circuits, when the choice: $\alpha=10$, $\beta=19$, $\gamma=0.1636$, $a=-1.4325$, $b=-0.7831$, and $\sigma=3$, $\varepsilon=0.5$, and $\tau=5.23$ was used. $k_1=k_2=k_3=5$ satisfy the stability (synchronization) condition (16), and $x(0)=(-1,-0.1,1)$ and $\xi(0)=(0,0,0)$. In the sequel, the same set of values will be used to obtain the numerical results.

5 Communicating with a single transmission channel

Figure 3 illustrates the communication scheme using a single transmission channel proposed in [20]. $m_o(t)$ denotes the confidential information and $m_r(t)$ the recovered information. $x_1(t)$ is a hyperchaotic state of (13),

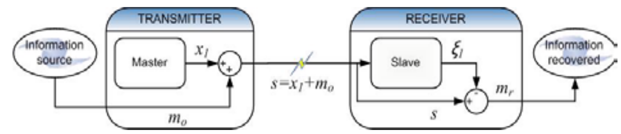

Figure 3: Hyperchaotic masking with a single transmission channel.

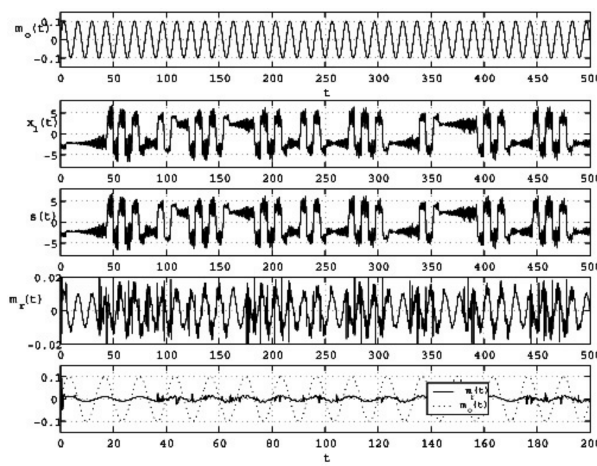

Figure 4: Transmission of confidential information using hyperchaotic encryption with a single transmission channel: $m_o(t)=0.1\sin(151t)$ and $m_r(t)$ the recovered information.

and is used to encrypt $m_o(t)$. So, the transmitted hyperchaotic signal to the receiver through a public channel is $s(t)=x_1(t)+m_o(t)$. At the receiver end, we obtain the signal $\xi_1(t)$, however $\xi_1(t)\approx x_1(t)$ so, the synchronization error is $e_1(t)=\xi_1(t)-x_1(t)\neq 0$, and as result $m_r(t)=m_o(t)+e_1(t)$.

We use as master/transmitter and slave/receiver to (13) and (14), respectively. Figure 4 shows the secure transmission using this communication scheme. We use like a confidential information a sinusoidal signal $m_o(t)=0.1\sin(151t)$; $x_1(t)$ is the hyperchaotic signal from (13) to encrypt $m_o(t)$; $s(t)=x_1(t)+m_o(t)$ the transmitted hyperchaotic signal, and $m_r(t)$ the recovered information. Note the evident error between signals $m_o(t)$ and $m_r(t)$.

6 Modified Communication scheme with a single transmission channel

The main problem with previous chaotic masking scheme is as follows. When the encrypted information is sent through $s(t)$, the states $\xi(t)$ of (14) do not synchronize

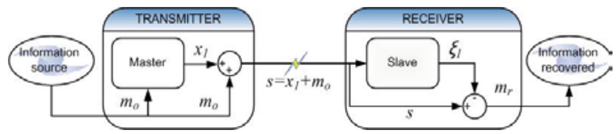

Figure 5: Modified hyperchaotic masking with a single transmission channel.

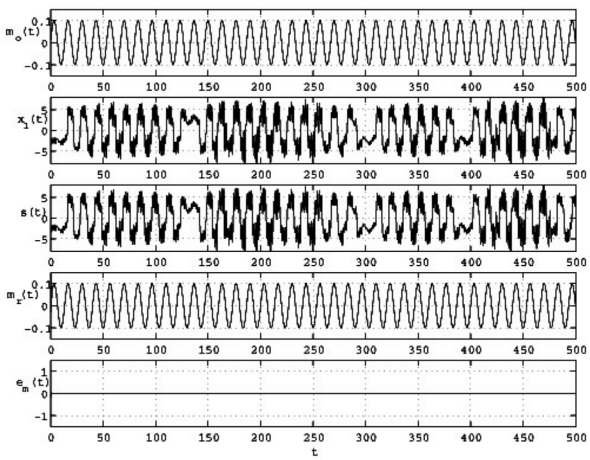

Figure 6: Transmission and exact recovery of confidential information $m_o\,(t) = 0.1 \sin(151t)$ by usisng modified scheme.

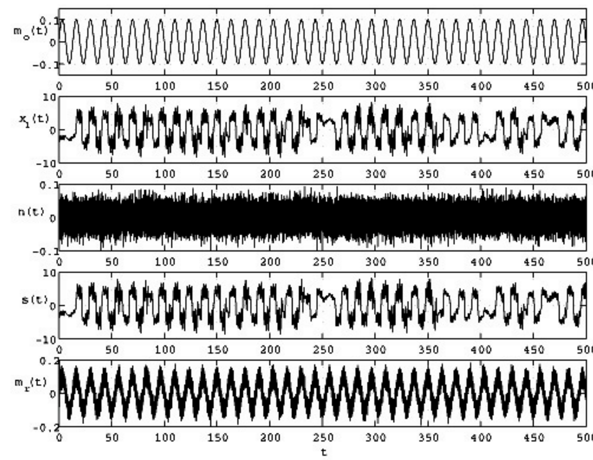

Figure 7: Transmission and recovery of confidential information $m_o\,(t) = 0.1 \sin(151t)$ through a noisy channel (by using modified scheme).

with the corresponding states $x\,(t)$ of (13). Thus, the confidential information is not recovered faithfully at the receiver end, and it is necessary a stage of low-pass filtering [20]; this is because the information $m_o\,(t)$ directly affects the dynamics of (14), and it is necessary that $m_o\,(t)$ be too small (in amplitude), such that, an approximate synchronization exists, because of that the additive information acts like an external perturbation in $s\,(t)$. While smaller it is, will be more possibilities of recovering the information. However, if additive noise is considered in the transmission channel, will be a difficult if not impossible task if the amplitude of $s\,(t)$ (including $m_o\,(t)$) is not large with respect to the noise level. We use the modified communication scheme shown in Fig. 5 proposed in [21, 22], here the sent information can be recovered faithfully without a of low-pass filtering stage, if there is not an additive noise present in the transmission channel, and it is not necessary that the information be too small to recovered process. If it is possible, then we can consider a noise level in the transmission channel, and to use a low-pass filter at the receiver end with the purpose to eliminate the noise effects only.

Due to transmitted signal $s(t) = y\,(t) + m_o(t)$, it is clear that $m_o\,(t)$ affects the dynamics of slave/receiver (14). From slave described by (3) the *slave/receiver* is now

$$\begin{aligned} \dot{\xi} &= \mathcal{J}(s)\frac{\partial H}{\partial \xi} + \mathcal{W}\frac{\partial H}{\partial \xi} + \mathcal{F}(s, s\,(t-\tau)) + K(s-\eta), \\ \eta &= \mathcal{C}\,\frac{\partial H}{\partial \xi}. \end{aligned} \tag{17}$$

If we need exact synchronization, i.e., $\xi(t) = x\,(t)$ as $t \to \infty$ for exact recovery of $m_o\,(t)$, then is necessary to modify the dynamics of the master (4). It is possible by feedback of $m_o(t)$ in the master (4). So, $m_o(t)$ also affects the dynamics of master in the same way that to receiver. Thus, from (4) the modified master/slave is described by

$$\begin{aligned} \dot{x} &= \mathcal{J}(s)\frac{\partial H}{\partial x} + \mathcal{W}\frac{\partial H}{\partial x} + \mathcal{F}(s, s\,(t-\tau)) + K(s-y), \\ y &= \mathcal{C}\,\frac{\partial H}{\partial x}. \end{aligned} \tag{18}$$

For time-delay-feedback Chua's circuit (11)-(12) with output $x_1(t)$; $m_o(t) = 0.1 \sin(151t)$, and $s(t) = x_1(t) + m_o(t)$. We have that the **master/transmitter** is described by

$$\begin{aligned} \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} \\ &\quad + \begin{bmatrix} -\alpha^2 & \alpha & 0 \\ \alpha & -1 & 0 \\ 0 & 0 & -\gamma\beta \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha f\,(s) \\ 0 \\ -\beta \sin(\sigma s\,(t-\tau)) \end{bmatrix} \end{aligned} \tag{19}$$

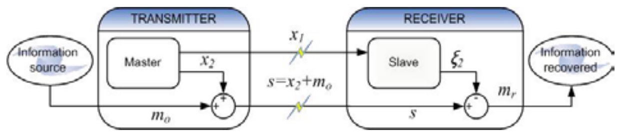

Figure 8: Hyperchaotic masking with two transmission channels.

and the corresponding **slave/receiver** given by

$$\begin{bmatrix}\dot{\xi}_1\\ \dot{\xi}_2\\ \dot{\xi}_3\end{bmatrix} = \begin{bmatrix}0 & 0 & 0\\ 0 & 0 & \beta\\ 0 & -\beta & 0\end{bmatrix}\frac{\partial H}{\partial \xi} + \begin{bmatrix}-\alpha^2 & \alpha & 0\\ \alpha & -1 & 0\\ 0 & 0 & -\gamma\beta\end{bmatrix}\frac{\partial H}{\partial \xi} \quad (20)$$

$$+\begin{bmatrix}-\alpha F(x_1)\\ 0\\ -\beta\sin(\sigma x_1(t-\tau))\end{bmatrix} + \begin{bmatrix}k_1\\ k_2\\ k_3\end{bmatrix} e_1.$$

Figure 6 shows the transmission of confidential information $m_o(t) = 0.1\sin(151t)$ using the modified scheme. The transmitted signal $s(t) = x_1(t)+m_o(t)$. The recovered information $m_r(t)$, Due to exact synchronization, it is possible faithfully recovering of $m_o(t)$, after synchronization time i.e., $e_m(t) = m_o(t) - m_r(t) = 0$.

Figure 7 shows the communication of $m_o(t)$ through noisy channel. The hyperchaotic signal $x_1(t)$, $n(t)$ is a noise signal presents in the transmission channel. Transmitted signal $s(t) = x_1(t) + m_o(t) + n(t)$. Recovered information $m_r(t)$. After a filtering stage we can obtain $e_m(t) = m_o(t) - m_r(t) = 0$.

7 Communicating with two transmission channels

With this scheme, we obtain faster synchronization and higher privacy; one channel is used to send the hyperchaotic synchronizing signal $x_1(t)$ from transmitter (13), with no connection with the confidential information $m_o(t)$. While other channel is used to transmit hidden information $m_o(t)$ which is recovered at the receiver end by means of the comparison between the signals $s(t) = x_2(t) + m_o(t)$ and $\xi_2(t)$. Figure 8 shows the hyperchaotic secure communication system with two transmission channels. Figure 9 illustrates the secure communication of confidential information $m_o(t)$ hidden through hyperchaotic signal $x_2(t)$ from (19), the transmitted hyperchaotic signal $s(t)$, the recovered information $m_r(t)$ at the receiver end which is obtained after a short transient behavior, and the error between $m_o(t)$ and $m_r(t)$, i.e., $e_m(t) = m_o(t) - m_r(t) = 0$.

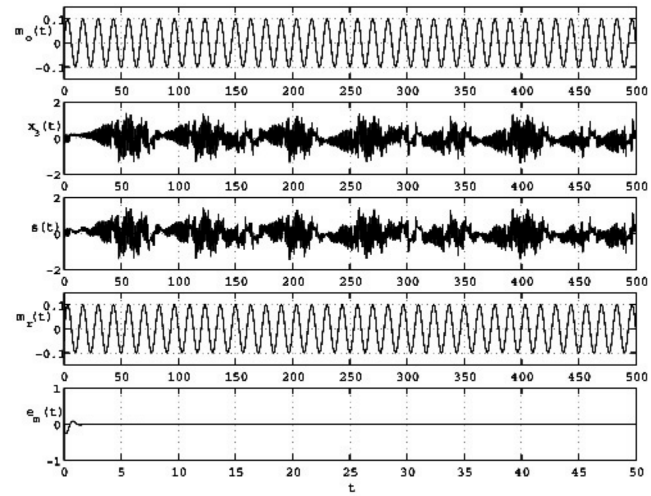

Figure 9: Transmission of $m_o(t) = 0.1\sin(151t)$ by using two transmission channels.

Figure 10 illustrates the transmission of $m_o(t) = 0.1\sin(151t)$ through a noisy channel. The hyperchaotic signal $x_2(t)$ encrypts $m_o(t)$; $n(t)$ is a noise signal presents in the transmission channel . Transmitted signal $s(t) = x_2(t)+m_o(t)+n(t)$. The recovered information $m_r(t)$ can be equal to original information $m_o(t)$ after filtering stage.

8 Conclusions

We have synchronized two time-delay-feedback Chua's circuits through the Generalized Hamiltonian forms and observer approach. Based on this synchronization property it is achieved secure transmission of confidential information. In addition, it is shown with two communication schemes the quality of the recovered information, and at the same time, we have increased the level of encryption security. The proposed communication schemes effectively repair the security flaws reported in the literature.

References

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

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

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

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

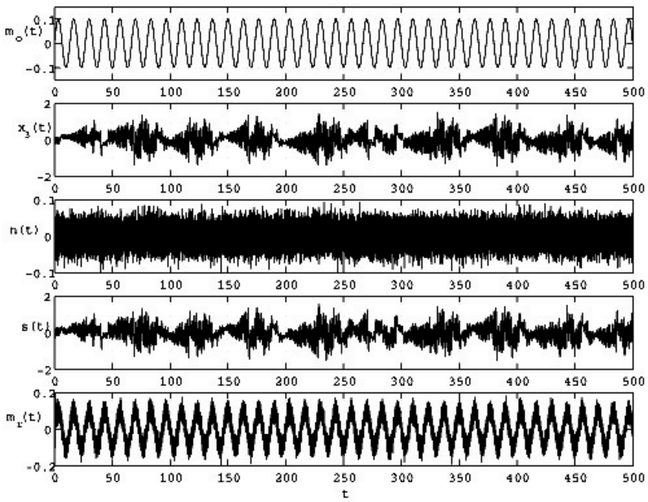

Figure 10: Transmission of $m_o(t) = 0.1 \sin(151t)$ through a noisy channel by using two transmission channels.

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

[6] D. López-Mancilla and C. Cruz-Hernández, Output synchronization of chaotic systems: Model-matching approach with application to secure communication, to appear in *Nonlinear Dynamics and Systems Theory* **5**(2) 2005.

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

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

[9] H. Serrano-Guerrero and C. Cruz-Hernández, *Procs. of the 2th Conferencia Internacional Automática*, Santiago de Cuba, Cuba 2002.

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

[11] J.H. Peng, E.J Ding, M. Ding, and W. Yang, Synchronizing hyperchaos with a scalar transmitted signal, *Phys. Rev. Lett.* **76**(6), 1996, 904-907.

[12] C. Cruz-Hernández, C. Posadas, and H. Sira-Ramírez, Synchronization of two hyperchaotic Chua circuits: A generalized Hamiltonian systems approach, *Procs. of the 15th IFAC World Congress*, July 21-26, 2002 Barcelona, Spain.

[13] A. Aguilar and C. Cruz-Hernández, Synchronization of two hyperchaotic Rössler systems: Model-matching approach, *WSEAS Trans. Systems* **1**(2) 2002 198-203.

[14] J.D. Farmer, Chaotic attractors of an infinite-dimensional dynamical systems, *Physica D*, **4**(2), 1982, 366-393.

[15] H. Lu and Z. He, Chaotic behaviors in first-order autonomous continuous-time systems with delay, *IEEE Trans. Circuits Syst. I*, **43**, 1996, 700-702.

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

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

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

[19] X.F. Wang, G.Q. Zhong, K.F. Tang, and Z.F. Liu, Generating chaos in Chua's circuit via time-delay feedback, *IEEE Trans. Circuits Syst. I*, **48**(9), 2001, 1151-1156.

[20] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogratz, Synchronization of Lorenz-based chaotic circuits with applications to communications, *IEEE Trans. Circuits Syst. II,* **40**(10) 1993 626-633.

[21] V. Milanović and M. E. Zaghloul, Improved masking algorithm for chaotic communication systems, *Electronics Lett.* **32**(1) 1996 11-12.

[22] D. López and C. Cruz-Hernández, A note on chaos-based communication schemes, to appear in *Revista Mexicana de Física* 2005.