Secret Communications Using Synchronized Sixth-Order Chua’s Circuits


Abstract—In this paper, we use Generalized Hamiltonian systems approach to synchronize a modified sixth-order Chua’s circuit, which generates hyperchaotic dynamics. Synchronization is obtained between the master and slave dynamics with the slave being given by an observer. We apply this approach to transmit private information (analog and binary), while the encoding remains potentially secure.

Keywords—hyperchaos synchronization; sixth-order Chua’s circuit; observers; simulation; secure communication.

I. INTRODUCTION

NOWAYS, information transmission plays a crucial role, where an ever-growing capacity for communication services are required. Two of the major requirements in communication systems are privacy and security.

Synchronization of chaotic systems, see e.g. [1]-[9] has been greatly motivated by the possibility of information encoding by using a chaotic carrier. First explored with electronic circuits, see e.g. [10]-[13], where a small signal (the confidential information) was added to a chaotic voltage and transmitted to a receiver circuit.

If chaotic synchronization is achieved between transmitter and receiver circuits, then with the chaotic carrier itself, and subtraction of the synchronized signal from the transmitted signal (carrier plus information signal) results in the recovery of the information.

From synchrony of chaotic systems, there is opened the potential application of this principle to construct systems for encryption that substitute the complicated conventional methods.

López-Gutiérrez R.M. is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México (corresponding author to provide phone: +52 646-175-0744; fax: +52 646-174-4333; (e-mail: rollopez@uabc.mx).

Rodríguez-Orozco E. is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México (e-mail: ron_ero@hotmail.com).

Cruz-Hernández C. is with the Electronics and Telecommunications Department, Scientific Research and Advanced Studies of Ensenada (CICESE), Ensenada B.C. 22860 México (e-mail: ceruz@cicese.mx).

Inzunza-González E. is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México, (e-mail: einzunza@uabc.mx).

Posadas-Castillo C. is with the Nuevo Leon Autonomous University (UANL); (e-mail: cpasadas@fime.unl.mx).

García-Guerrero E. E. is with the Baja California Autonomous University (UABC), Ensenada, B.C. 22860 México; (e-mail: egarcia@uabc.mx).

Cardoza-Avendaño L. is with the Baja California Autonomous University (UABC); (e-mail: lcardoza@uabc.mx).

The rest of this paper is arranged as follows: in Section II a summary on synchronization of chaotic systems in Generalized Hamiltonian forms is given. In Section III, the hyperchaotic Chua’s circuit (sixth-order) is described. In Section IV, the synchronization of two hyperchaotic Chua’s circuits is shown. In Section V, stability conditions are presented. In the Section VI an application to encoding, transmission, and decoding is given. Finally, in Section VII some concluding remarks are given.

II. CHAOTIC SYNCHRONIZATION VIA GENERALIZED HAMILTONIAN SYSTEMS

Consider the following n-dimensional system

\[ \dot{x} = f(x), \quad x(t) \in \mathbb{R}^n \]

which represent a model exhibiting hyperchaotic behavior. Following the approach provided in [Sira-Ramírez y Cruz-Hernández, 2001], many physical systems described by Eq. (1) can be written in “Generalized Hamiltonian” canonical form,

\[ \dot{x} = J \left( x \right) \frac{\partial H}{\partial x} + S( x ) \frac{\partial H}{\partial \dot{x}} + F( x ), \quad x \in \mathbb{R}^n, \]

where \( H(x) \) denotes a smooth energy function which is globally positive definite in \( \mathbb{R}^n \). The gradient vector of \( H \), denoted by \( \partial H/\partial \dot{x} \), is assumed to exist everywhere. We use...
The matrices, \( J(\cdot) \) and \( S(\cdot) \), satisfy, for all \( x \neq 0 \), the properties: \( J(\cdot) \cdot J(\cdot) = I \) and \( S(\cdot) = S(\cdot)^{T} \). The vector field \( J(\cdot) \partial H / \partial x \) exhibits the conservative part of the system and it is also referred to as the workless part, or work-less forces of the system; and \( S(x) \) depicting the working or nonconservative part of the system. For certain systems, \( S(\cdot) \) is negative definite or negative semidefinite. Thus, the vector field is considered as the dissipative part of the system. If, on the other hand, \( S(\cdot) \) is positive definite or negative semidefinite, the system is considered as the dissipative part of the system. If, in this case, we can always (although nonuniquely) decompose the system into a symmetric negative definite or negative semidefinite matrix, and a symmetric positive semidefinite matrix (Krstic et al., 1995). Finally, \( f(\cdot) \) represents a locally destabilizing vector field.

In the context of observer design, we consider a special class of Generalized Hamiltonian forms with linear output map \( y(t) \), given by

\[
\dot{x} = J(y) \frac{\partial H}{\partial x} + (1 + S) \frac{\partial H}{\partial x} + F(y), \quad x \in \mathbb{R}^{n},
\]

\[
y = C \frac{\partial H}{\partial x}, \quad y \in \mathbb{R}^{m},
\]

where \( S \) is a constant symmetric matrix, not necessarily of definite sign. The matrix \( J \) is a constant skew symmetric matrix. The matrix \( C \) is a constant matrix.

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

\[
\dot{\tilde{x}} = J(y) \frac{\partial H}{\partial x} + (1 + S) \frac{\partial H}{\partial x} + F(y) + K(y - \eta), \quad \tilde{x} \in \mathbb{R}^{n},
\]

\[
\eta = \frac{\partial H}{\partial \epsilon}, \quad \eta \in \mathbb{R}^{m}
\]

\( K \) is the observer gain.

The state estimation error, defined as \( e(t) = x(t) - \tilde{x}(t) \) and the output estimation error, defined as \( e_{y}(t) = y(t) - \eta(t) \) are governed by

\[
\dot{e} = J(y) \frac{\partial H}{\partial \epsilon} + (1 + S - KC) \frac{\partial H}{\partial \epsilon} + F(y) + K(y - \eta), \quad e \in \mathbb{R}^{n},
\]

\[
e_{y} = C \frac{\partial H}{\partial \epsilon}, \quad e_{y} \in \mathbb{R}^{m},
\]

where the vector \( \partial H / \partial \epsilon \) actually stands, with some abuse of notation, for the gradient vector of the modified energy function, \( \partial H(e) / \partial \epsilon = \partial H / \partial x - \partial H / \partial \epsilon = M \). When \( (K + S) = \mathbf{W} \).

Definition 1 (Chaotic synchronization) (Liu, 2000) The slave system (4) (nonlinear state observer) synchronizes with the chaotic master system in the special class of Generalized Hamiltonian form (3), if

\[
\lim_{t \to \infty} \left\| x(t) - \tilde{x}(t) \right\| = 0
\]

no matter which initial conditions \( x(0) \) and \( \tilde{x}(0) \) have.

A necessary and sufficient condition for global asymptotic stability to zero of the estimation error (5) is given by the following theorem.

Theorem 1 (Liu, 2000) The state \( x(t) \) of the nonlinear system (3) can be globally, exponentially, asymptotically estimated, by the state \( \tilde{x}(t) \) of the observer (4) if and only if, there exists a constant matrix \( K \) such that the symmetric matrix

\[
[W - KQ + |W - KQ|^2 = |S - KQ| + |S - KQ|^2 = 2|S - \frac{1}{2}(KC + C'K')|
\]

is negative definite.

III. HYPERCHAOTIC CHUA CIRCUIT (SIXTH-ORDER)

Consider the modified sixth-order Chua’s circuit described by [Suykens et al., 1997]:

\[
\begin{align*}
\dot{x}_1 &= \alpha [x_1 - h(x_1)] + \beta x_2, \\
\dot{x}_2 &= x_1 - x_3 + x_5, \\
\dot{x}_3 &= -\beta x_2, \\
\dot{x}_4 &= \alpha [x_1 - h(x_1)] + K_p(x_4 - x_1), \\
\dot{x}_5 &= x_4 - x_3 + x_6, \\
\dot{x}_6 &= -\beta x_5,
\end{align*}
\]

with nonlinear function given by

\[
h(x_1) = \sum_{i=1}^{n} m_i (x_1 - c_i)(x_1 - c_i) + \sum_{i=1}^{n} m_i (x_1 - c_i)
\]

where \( n = 3, K_p = 0.01, \alpha = 9, \beta = 14.28, m = [0.9/7, -3/7, 3.5/7, 2.7/7, 4/7, -2.4/7, 1, 2.15, 3.6, 6.2, 9], \) and \( c = [1, 0.9/7, -3/7, 3.5/7, 2.7/7, 4/7, -2.4/7] \), the modified sixth-order Chua’s circuit (7)-(8) exhibits hyperchaotic behavior, with two positive Lyapunov exponents. Figure 1 shows the attractor points \( x_1, x_2, x_3, x_4, x_5, x_6 \) and \( x_1, x_2, x_3, x_4, x_5, x_6 \).
The destabilizing vector field calls for used as the outputs of the master circuit (10). The matrices \(C, S, \) and \(I\) are given by

\[
C = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 \end{bmatrix},
\]

\[
S = \begin{bmatrix} 0 & \alpha & 0 & -\frac{K_p}{2} & 0 \\ \alpha & 0 & 0 & 0 & 0 \\ -\frac{K_p}{2} & 0 & 0 & \alpha & 0 \\ 0 & 0 & \alpha & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},
\]

\[
I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ -\alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\beta & 0 \\ 0 & 0 & 0 & 0 & -\beta \end{bmatrix}.
\]

The nonlinear state observer (slave circuit) for (ID) is designed as

\[
\begin{align*}
\dot{\hat{x}}_1 & = \frac{1}{2} \left( -K_p \alpha \hat{x}_1 + K_{\alpha 2} \right) + \frac{1}{2} \beta \hat{x}_4 + \hat{x}_5, \\
\dot{\hat{x}}_2 & = \frac{1}{2} \left( -K_p \alpha \hat{x}_2 + K_{\alpha 4} \right) + \frac{1}{2} \beta \hat{x}_6 + \hat{x}_7,
\end{align*}
\]

\[\begin{cases}
\dot{e}_y = \left[ \begin{array}{c}
\dot{x}_1 - \hat{x}_1 \\
\dot{x}_2 - \hat{x}_2
\end{array} \right],
\end{cases}
\]

where the error is \( e_y \). From (ID) and (II) we have that the synchronization error dynamics is governed by

\[
\begin{align*}
\dot{e}_y & = \left[ \begin{array}{c}
\dot{x}_1 - \hat{x}_1 \\
\dot{x}_2 - \hat{x}_2
\end{array} \right],
\end{align*}
\]

One may now choose the observer gain \( K = (k_1, k_2, k_3, k_4, k_5, k_6)^T \) in order to guarantee asymptotic exponential stability to zero of the synchronization error \( e(t) = x(t) - \hat{x}(t) \), as will be shown in next section.

V. STABILITY CONDITIONS

In this section, we examine the stability of the synchronization error (12) between the master (10) in Hamiltonian form and slave (11) nonlinear state observer. Invoking to Theorem 1 and applying the Sylvester’s criterion - which provides a test for negative definite of a matrix- thus, we have that the matrix \( 2[S-(1/2)(KC+C^T K^{-1})] \) will be negative definite matrix, if we choose \( k_1, k_2, k_3, k_4, k_5, \) and \( k_6 \) such that the following condition are satisfied:
For next numerical simulations, we have used the gains $k_3$, $k_4$, and $k_6$ are equal to zero, $k_1 = 1$, $k_2 = 2$, and $k_4 = 1.82$. The initial conditions: $x(0) = (0.1, 0.1, 0.1, 0.1, 0.1, 0)$. Fig. 2 shows the synchronization between master (10) and slave (11) with sixth-order Chua’s circuits.

\[
\begin{align*}
-2K_4\alpha & \leq 0 \\
4K_2 - K_2^2 & \leq 4.44 \\
2K_1^2 & \leq 0 \\
-4K_3^2 & \leq 0 \\
4K_5 - K_5^2 & \leq 4.00049 \\
K_6 & = 0
\end{align*}
\]

Fig. 2. Synchronization between hyperchaotic Chua’s circuits (10) and (11).

VI. APPLICATION TO ENCODING, TRANSMISSION, AND DECODING

Synchronization of two six-order Chua’s circuits allows us to design secret communication systems, where the confidential information is hidden into the transmitted hyperchaotic signal. In this paper, we present two cases, encoding, transmission, and decoding of analog and binary signals.

A. Transmission of analog message

Two channels are used to synchronize master and slave modified Chua’s circuits (10) and (11) via coupling hyperchaotic signals $x_3(t)$ and $x_4(t)$. Meanwhile, the other channel is used to transmit hidden message $m(t) = 0.01 \sin(t)$ (see Fig. 4), which is added to signal $x_3(t)$ of the transmitter $Tx$, the transmitted signal to receiver $Rx$ is $s(t)$. At the receiver end, the recovered message $m'(t)$ is given.

The information signal $m(t)$ is added to channel $x_3(t)$ of the transmitter $Tx$ (Fig.5a). The transmitted signal $s(t)$ (Fig. 5b)) is received the receiver end $Rx$. The signal $s(t)$ is subtracted to the output $\hat{x}_3(t)$ generates in $Rx$, then we recovery the information $m'(t)$ (see Figure 5c). Finally, Fig. 5d shows the error between original and recovered messages.

Fig. 4. Secret communication scheme to transmit analog messages.

B. Transmission of binary message

The binary message $m(t)$ (see Fig. 6) is modulated by using the parameter $\alpha$. By commutating from $\alpha = 9$ (for encoding a “0” bit) to $\alpha' = 13$ (for encoding a “1” bit). The state signals $x_1(t)$ and $x_4(t)$ are used to synchronize transmitter and receiver, moreover is possible to recovery the message using parametric commutation. This technique is based on if there exists synchrony or not.

Fig. 5. (a) Confidential message, (b) transmitted hyperchaotic signal, (c) recovered message, and (d) error between original and recovered messages.

Fig. 6 Secret communication scheme to transmit binary messages.
Figure 7 shows the encoding, transmission, and decoding of binary signal. Fig. 7(a) shows the original binary message. Fig. 7(b) shows the hyperchaotic transmitted signal, and Fig. 7(c) shows the recovered binary message.

VII. CONCLUSION

In this work, we have synchronized hyperchaotic dynamics in a modified sixth-order Chua’s circuit through the Generalized Hamiltonian forms and observer approach. Based on this synchronization property, it is achieved secret transmission of confidential information. In addition, it has been shown the quality of the recovered information, and at the same time, we have increased the encryption security by using extremely complex dynamics.

We overcame the low security objections against low dimensional chaos-based communication schemes, we confronted two problems: make the transmitted signal more complex, and reduce the redundancy in the transmitted signal. To achieve the first goal, it was necessary to use hyperchaos to generate very complex transmitted signals by using a modified sixth-order Chua’s circuit.

To achieve the second goal, Generalized Hamiltonian forms and observer methodology for hyperchaos synchronization offers a very promising approach. The approach can be implemented on experimental setup, and shows great potential for actual communication systems in which the encoding is required to be secure.

ACKNOWLEDGMENT

The authors would like to thank to CONACYT, México by the support under Research Grants Nos. J49593-Y and P50051-Y. And to UABC, México, by academic mobility.

REFERENCES


López-Gutiérrez R. M. was born in 10-11-1972. She is a Professor of Electronics Engineering in Baja California Autonomous University since 2001. She received her Master Science degree and Ph.D. degree in Electronics and Telecommunications from CICESE, México in 1996 and 2003, respectively. Her research interests involve synchronization of complex systems and applications.

Cruz Hernández C. received the M.S. and Ph.D. degrees in electrical engineering from CINVESTAV, México, in 1991 and 1995, respectively. Since 1995, he is with the Department of Electronics and Telecommunications of the Scientific Research and Advanced Studies of Ensenada (CICESE), where, he is current Professor of Automatic Control. His research interests
include multimode oscillations of coupled oscillators, nonlinear systems analysis, and synchronization and control of complex dynamical systems.

**Inzunza González E.** was born in Navolato, Sinaloa México on 1976. Received the Bachelors degree in Electronic Engineer from the Culiacán Institute of technology, in 1999, the M. Sc. degree in electronics and telecommunications from CICESE, México, in 2001. Since August 2008, he where, he is current Professor of Automatic Control. His research interests include multimode oscillations of coupled oscillators, nonlinear systems analysis, and synchronization and control of complex dynamical systems.

**Posadas-Castillo C.** was born in Poza Rica, Veracruz, México; in March 10 of 1973. He received the Engineer Degree in Control and Computation from the Autonomous University of Nuevo León, in 1997, Master in Science Degree in Electronics and Telecommunications, from CICESE in 2001, and Ph.D. degrees in electrical from Baja California Autonomous University, in 2008. Since 1997, he has been Associated Professor of the University Autonomous of Nuevo León, México. His research interests include synchronization and control of complex systems, nonlinear systems analysis, and private communications.

**Garcia-Guerrero E. E.** studied physics engineering at the University Autonomous Metropolitana, Mexico, and received the PhD degree in optical physics from the Scientific Research and Advanced Studies Center of Ensenada, B.C, (CICESE) Mexico. He has been with the Engineering Faculty, Baja California Autonomous University (UABC) Mexico since 2004. His current interests are in the field of Optical Synchronization of Complex Systems.

**Cardoza-Avendaño L.** was born in Ensenada, B.C. México on 1980. She is Professor of Electronics Engineering in Baja California Autonomous University since 2005. She received her Master Engineering degree in Electrical Engineering from Baja California Autonomous University, México, in 2008. Since August 2008, she has been a PhD student. Her research interests involve synchronization of complex systems and Applications.