Abstract—In this paper, encrypted audio communications based on synchronization of coupled unified chaotic systems in master-slave configuration is numerically studied. We transmit the encrypted audio messages by using two insecure channels. Encoding, transmission, and decoding audio messages in chaotic communication is presented.

Keywords—Audio Encrypted, Chaos, Synchronization

I. INTRODUCTION

During the last decades, synchronization of two coupled chaotic systems has received great attention from mathematicians, physicists, biologists, control engineers, etc. see e.g. [1]-[7]. This interest has been greatly motivated by the possibility of encrypted information transmission by using a chaotic carrier, see e.g. [4, 8-14].

Based on chaos synchronization of two unified systems reported in [15], the aim of this paper is to study the encrypted audio transmission. In particular, this objective is achieved by synchronizing the unified chaotic systems via Generalized Hamiltonian forms and observer design proposed in [5]. Recently, was shown in [15] that the mentioned approach is indeed suitable to synchronize two coupled unified chaotic systems in master-slave configuration. In this work, we transmit encrypted audio messages via insecure channels between two remote points.

The present study shows the encrypted and recovery of audio messages by using two unified systems. In particular, when Lorenz-Lorenz, Chen-Chen, and Lü-Lü chaotic systems are operated.

The remainder of this paper is organized as follows: In Section II, the system communication description is given. In Section III, the model of the unified chaotic system is described. Section IV presents the synchronization of two unified chaotic systems by using Hamiltonian forms and observer approach. In Section V, encrypted audio transmission is shown. The paper is concluded with some remarks in Section VI.

Encrypted audio communication based on synchronized unified chaotic systems


II. SYSTEM COMMUNICATION DESCRIPTION

In this section, a cryptosystem based on synchronized chaotic systems is described. The aim is to transmit encrypted audio messages from transmitter A to remote receiver B as is depicted in Fig. 1. An audio message $m$ is to be transmitted over an insecure communication channel. To avoid any unauthorized receiver (intruder $O$) located at the mentioned channel; $m$ is encrypted prior to transmission to generate an encrypted message $c$,

$$c = e(m,k),$$

by using a chaotic system $e$ on transmitter A.

The encrypted message $c$ is sent to receiver B, where $m$ is recovered as $\hat{m}$ from the chaotic decryption $d$, as

$$\hat{m} = d(c,k).$$

If $c$ and $d$ have used the same key $k$, then at receiver end B it is possible to obtain $\hat{m} = m$. A secure channel (dashed line) is used for transmission of the keys, $k$. Generally, this secure communication channel is a courier and is too slow for the transmission of $m$. Our chaotic cryptosystem is reliable, if it preserves the security of $m$, i.e. if $m' \neq m$ for even the best cryptanalytic function $h$, given by

$$m' = h(c).$$

To achieve the proposed chaotic encryption scheme, we appeal to unified chaotic system for encryption/decryption purposes ($e$ and $d$, respectively).

The unified chaotic system have a number of parameters determining their dynamics; such parameters and initial conditions are the coding “keys”, $k$. We expect that it can perform the objective of the secure communication and the transmitting audio messages can be recovered at the receiver B. In order to guarantee the encryption and decryption, the unified chaotic systems have to achieve the so-called synchronization on both chaotic transmitter A and receiver B.
III. Unified Chaotic System

Consider the unified chaotic system [16], described by

\[
\begin{align*}
\dot{x}_1 &= (25\alpha + 10) (x_2 - x_1), \\
\dot{x}_2 &= (28 - 35\alpha) x_1 - x_1 x_3 + (29\alpha - 1) x_2, \\
\dot{x}_3 &= x_1 x_2 - \left( \frac{\alpha + 8}{3} \right) x_3,
\end{align*}
\]

where the parameter \( \alpha \in [0, 1] \), for the whole interval the unified system is chaotic. Obviously, when \( \alpha = 0 \) the system (1) is the original Lorenz system [17]. While for \( \alpha = 1 \) the system (1) is the original Chen system [18]. For \( \alpha = 4/5 \) the system (1) corresponds to the critical (Lü) system [19]. In fact, the system (1) bridges the gap between the Lorenz and Chen systems [16].

By using the initial conditions \( x(0) = (0.1, 0.1, 0.01) \), Figs. 2, 3, and 4 show the chaotic attractors of Lorenz, Chen, and Lü respectively, projected onto \((x_1, x_2, x_3)\)-space.

IV. Synchronization of Two Unified Chaotic Systems

Considering the following chaotic system described by the state equation

\[
\dot{x} = f(x),
\]

where \( x \in \mathbb{R}^n \) is the state vector, \( f : \mathbb{R}^n \rightarrow \mathbb{R}^n \) is a nonlinear function. In [5] was reported how the chaotic system (2) can be rewritten in the following Generalized Hamiltonian canonical form,

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

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

\[
\begin{align*}
\dot{x} &= J(y) \frac{\partial H}{\partial x} + (I + S) \frac{\partial H}{\partial x} + F(y), \quad x \in \mathbb{R}^n, \\
y &= C \frac{\partial H}{\partial x}, \quad y \in \mathbb{R}^m.
\end{align*}
\]

Denoting the estimate of the state \( x \) by \( \xi \), and considering the Hamiltonian energy function \( H(\xi) \) to be the particularization of \( H \) in terms of \( \xi \). Similarly, we denote by \( \eta \) the estimated output, computed in terms of the estimated state \( \xi \).

A nonlinear state observer for the special class of Generalized Hamiltonian form (4) is given by

\[
\begin{align*}
\dot{\xi} &= J(y) \frac{\partial H}{\partial x} + (I + S) \frac{\partial H}{\partial x} + F(y) + K(y - \eta), \\
\dot{\eta} &= C \frac{\partial H}{\partial x}, \quad \eta \in \mathbb{R}^m,
\end{align*}
\]

with \( \xi, \eta \in \mathbb{R}^n \) and \( K \) is the observer gain.

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

\[
\begin{align*}
\dot{e} &= J(y) \frac{\partial H}{\partial x} + (I + S - KC) \frac{\partial H}{\partial x}, \quad e \in \mathbb{R}^n, \\
\dot{e}_y &= C \frac{\partial H}{\partial x}, \quad e_y \in \mathbb{R}^m.
\end{align*}
\]

Definition 1 (Chaotic synchronization) [7]. The slave system (5) (nonlinear state observer) synchronizes with the chaotic master system in the special class of Generalized Hamiltonian form (4), if

\[
\lim_{t \to \infty} \| x(t) - \xi(t) \| = 0,
\]

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.

In the sequel, we synchronize two unified chaotic systems (1) in master-slave configuration (see Fig. 5), via Generalized Hamiltonian forms and observer design proposed in [5]. Firstly, we rewrite the unified system (1) in Hamiltonian form as the master system and design a state observer for (1) like the slave system, as follows. Taking as Hamiltonian energy function to
\[ H(x) = \frac{1}{2} \left( x_1^2 + x_2^2 + x_3^2 \right) \]  

and gradient vector as

\[
\frac{\partial H}{\partial x} = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
x_1 \\
x_2 \\
x_3 \\
\end{bmatrix} = \begin{bmatrix}
x_1 \\
x_2 \\
x_3 \\
\end{bmatrix}.
\]

The unified system (1) in Hamiltonian form according to Eq. (4) (as master system) is given by

\[
\begin{bmatrix}
\dot{x}_1 \\
\dot{x}_2 \\
\dot{x}_3 \\
\end{bmatrix} = \begin{bmatrix}
0 & 30\alpha - 9 & 0 \\
-(30\alpha - 9) & 0 & -x_3 \\
0 & 0 & 0 \\
\end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix}
-(25\alpha + 10) & -5\alpha + 19 & 0 \\
-5\alpha + 19 & 29\alpha - 1 & 0 \\
0 & 0 & 0 \\
\end{bmatrix} \frac{\partial H}{\partial x}.
\]

The output signal to be transmitted to slave system is \( y = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x} = x_1 \). The matrices \( C \), \( S \), and \( I \), are given by

\[
C = \begin{bmatrix}
1 & 0 & 0 \\
\end{bmatrix},
\]
\[
S = \begin{bmatrix}
-(25\alpha + 10) & -5\alpha + 19 & 0 \\
-5\alpha + 19 & 29\alpha - 1 & 0 \\
0 & 0 & 0 \\
\end{bmatrix},
\]
\[
I = \begin{bmatrix}
-(30\alpha - 9) & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}.
\]

In [15] was shown that the pair of matrices \( (C,S) \) constitutes a pair detectable, but non observable. Thus, it is possible to design an observer for master system (10) (as slave system) according to Eq. (5), is as follows

\[
\begin{bmatrix}
\dot{\xi}_1 \\
\dot{\xi}_2 \\
\dot{\xi}_3 \\
\end{bmatrix} = \begin{bmatrix}
0 & 30\alpha - 9 & 0 \\
-(30\alpha - 9) & 0 & -y \\
0 & y & 0 \\
\end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix}
-(25\alpha + 10) & -5\alpha + 19 & 0 \\
-5\alpha + 19 & 29\alpha - 1 & 0 \\
0 & 0 & 0 \\
\end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix}
k_1 \\
k_2 \\
k_3 \\
\end{bmatrix} e_1,
\]

\[ \eta = \xi_1, \]

where the synchronization error is defined as \( e_1 = y - \eta \). From (10) and (11) the synchronization error dynamics is governed by

In [15] was given the stability conditions which guarantees asymptotic stability to zero of \( c(t) \) Eq. (12). Based on the mentioned conditions, we have selected \( k_1 = 11 \), \( k_2 = 50 \), and \( k_3 = 32 \) which guarantee the convergence of the synchronization error Eq. (12) to zero.

V. ENCRYPTED AUDIO COMMUNICATION

In this section, we describe the communication system based on synchronized chaos. Fig. 6 shows a block diagram to transmit secret audio messages by chaotic additive masking technique. We will use the unified system (1) as chaos generator. With this scheme, we obtain faster synchronization and higher privacy; one channel is used to send the chaotic synchronizing signal \( x_1(t) \) from the transmitter (10), with no connection with the secret audio message \( m(t) \). While the other channel is used to transmit hidden message \( m(t) \) which is recovered at the receiver end by means of the comparison between the signals \( x_2(t) + m(t) \) and \( \xi_2(t) \). Figure 6 shows the chaotic secure communication system with two transmission channels.

In this final part, via numerical simulations, we illustrate the encrypted audio transmission. We use as transmitter and receiver the unified chaotic system given in (1), for different values of parameter \( \alpha \), i.e. for Lorenz (\( \alpha = 0 \)), Chen system (\( \alpha = 1 \)), and Lü chaotic system (\( \alpha = 4/5 \)), and for initial conditions \( x(0) = (0.25, 0.3, 0.15) \) and \( \xi(0) = (0.1, 0.2, 0.25) \). The format of the audio signal \( m(t) \) is PCM 22.05 KHz, 16 Bits, monofonic channel. The mentioned audio message \( m(t) \) is to be encrypted and transmitted to the receiver.

Fig. 7 shows audio communication via Lorenz-Lorenz systems (\( \alpha = 0 \)). Original audio message \( m(t) \) to be encrypted and transmitted (top of figure), transmitted chaotic signal \( c(t) = x_2(t) + m(t) \) (middle of figure), and recovered audio message \( \hat{m}(t) \) (bottom of figure).

Fig. 8 shows audio communication by using Chen-Chen systems (\( \alpha = 1 \)). Original audio message \( m(t) \) to be encrypted.
and transmitted (top of figure), transmitted chaotic signal $c(t) = x_2(t) + m(t)$ (middle of figure), and recovered audio message $\hat{m}(t)$ (bottom of figure).

Fig. 9 shows audio communication by using Lü-Lü systems ($\alpha = 4/5$). Original audio message $m(t)$ to be encrypted and transmitted (top of figure), transmitted chaotic signal $c(t) = x_2(t) + m(t)$ (middle of figure), and recovered audio message $\hat{m}(t)$ (bottom of figure).

Fig. 10 shows audio communication by using Lorenz system as transmitter and the Chen system as receiver. Original audio message $m(t)$ to be encrypted and transmitted (top of figure), transmitted chaotic signal $c(t) = x_2(t) + m(t)$ (middle of figure), and recovered audio message $\hat{m}(t)$ (bottom of figure).

Fig. 11 shows audio communication by using the Lorenz system as transmitter and Lü system as receiver. Original audio message $m(t)$ to be encrypted and transmitted (top of figure), transmitted chaotic signal $c(t) = x_2(t) + m(t)$ (middle of figure), and recovered audio message $\hat{m}(t)$ (bottom of figure).

Fig. 12 shows Lü system as transmitter and Chen system as receiver. Original audio message $m(t)$ to be encrypted and transmitted (top of figure), transmitted chaotic signal $c(t) = x_2(t) + m(t)$ (middle of figure), and recovered audio message $\hat{m}(t)$ (bottom of figure).
In this paper, we have presented the transmission of encrypted audio messages based on synchronization of unified chaotic systems. This work have shown that the proposed chaotic communication schemes show a great potential for actual encryption communication systems in which the encoding is required to be secure. In a forthcoming article we will be concerned with a physical implementation of the synchronization of two chaotic unified systems in master-slave configuration, and its application to private communication of audio transmission in a network of users.

**REFERENCES**


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.

López-Gutiérrez R. M. was born on 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, Mexico in 1996 and 2003, respectively. Her research interests involve synchronization of complex systems and applications.

Serrano-Guerrero H. was born in Culiacán, Sinaloa, México. Received the Bachelors degree in electronic engineer from the Culiacán Institute of technology in 2000, the M. Sc. degree in instrumentation and control from CICESE, México, in 2002. From March 2003 to August 2006 he worked as Test Engineer in Electrónica Lowrance de México. From August 2006 to August 2008 he was a full time professor in the Faculty of Engineering of the Universidad Autónoma de Baja California, México. Since August 2008, he has been a doctoral student and subject professor in the Faculty of Engineering of the Universidad Autónoma de Baja California, México. His current research interest includes control and synchronization of complex dynamical systems, and encrypted transmissions using chaos.

García-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.