Synchronization of fractional-order Lü chaotic oscillators for voice encryption

O. García-Sepúlveda, C. Posadas-Castillo, A.D. Cortés-Preciado, M.A. Platas-Garza, and E. Garza-González
Universidad Autónoma de Nuevo León; Facultad de Ingeniería Mecánica y Eléctrica,
San Nicolás de los Garza, México.
e-mail: otoniel.garciasp@uanl.edu.mx; cornelio.posadascs@uanl.edu.mx; alfredo.cortespr@uanl.edu.mx;
miguel.platasgrz@uanl.edu.mx; eliezer.garzagzz@uanl.edu.mx

Allan G. S. Sánchez
Consejo Nacional Ciencia y Tecnología, Instituto Tecnológico de Celaya,
Antonio García Cubas Pte. 600, 38010, Celaya, Gto., México.
e-mail: allan.soriano@itcelaya.edu.mx

Received 12 September 2019; accepted 11 October 2019

In this paper, the encryption improvement via modulation of the fractional-order chaotic oscillators state variables is presented. A network of N-coupled fractional-order Lü chaotic oscillators, is synchronized. A voice message is encrypted, via additive encryption, by using a state variable of the synchronized network. The selected state variable is modulated and used to encrypt the message again. The results are compared.

Keywords: Non-linear systems; fractional order; chaos; synchronization; encryption; modulation.

En este artículo, se presenta la mejora de la calidad de encriptado mediante la modulación de las variables de estado de osciladores caóticos de orden fraccionario. Se sincroniza una red de N osciladores caóticos Lü de orden fraccionarios acoplados. Se encripta un mensaje de voz mediante encriptado aditivo, utilizando una variable de estado de la red sincronizada. La variable de estado seleccionada se modula y se utiliza para cifrar el mensaje nuevamente. Se comparan los resultados.

Descriptores: Sistemas no lineales; orden fraccionario; caos; sincronización; encriptado; modulación.

PACS: 05.45.-a; 05.45.Gg; 05.45.Pq; 05.45.Vx; 05.45.Xt DOI: https://doi.org/10.31349/RevMexFis.66.364

1. Introduction

In this document, an alternative way to improve a voice encryption quality is addressed. Some terms as fractional-order oscillators, chaos, complex networks, synchronization, data encryption and state variables modulation are shown. It is recommended to the reader interested in deepening on these topics to read [1–4].

The word *chaos* derives from the greek word $\chi\alpha o\sigma$, commonly associated with disorder, irregularity, or erratic behaviors [2]. In 1963, Edward Lorenz, an American mathematician and meteorologist, discovered one of the principles of complexity, the chaos. During his research, he observed that the climate exhibits a non-linear behavior known as a sensitive dependence to initial conditions. Using a mathematical model to forecast the behavior of the climate, showed that starting from two nearby points, the trajectories of the system that is currently known as *the Lorenz system*, diverge rapidly. He explained that this phenomenon makes impossible the long-term weather forecast. Time later, it was known as the butterfly effect [2].

Due to their chaotic nature, the chaotic oscillators are sensitive to their initial conditions, generating apparently random. However, chaos is deterministic [2]. This makes possible to replicate their behavior, if the initial conditions are known. This feature can be used in a secure communication scheme to confuse the attackers.

In a transmitter-receiver communication scheme, it is important to ensure that the initial conditions of the receiver are identical to those of the transmitter in time. If this is not guaranteed, the recovery of the encrypted message can be partial or null.

This is due to the sensitive dependence on the initial conditions presented by the chaotic systems. To guarantee the correct recovery of the message, establishing a communication system that transmits the dynamics of the transmitter in the receiver is needed. This can be achieved by synchrony effect. This phenomenon is responsible for homogenizing the independent dynamics of each oscillator.

The term *synchrony* meaning "with, at the same time" comes from the Greek $\sigma\acute{\upsilon}\nu$ "with" and from the Greek mythology $\chi\rho\acute{o}\nu o\varsigma$ "time". Synchrony, refers to the fact that two different behaviors will be equal in time, if there exists a coupling medium. In 1990, Pecora & Carrol, managed to synchronize two identical chaotic systems with different initial conditions, proving the synchrony phenomenon [5]. On the other hand, in order to synchronize non-identical systems, the existence of a generalized synchronization between coupled systems has been studied [6]. Furthermore, the chaos synchronization has been demonstrated by several physical implementations, *e.g.*, [7, 8].

In this paper, the synchronization between N non-integer order identical systems, commonly known as fractional-order systems, is achieved. These systems can be coupled in a

complex network that can be defined as an interconnected set of oscillators (two or more).

It is important to mention, that the fractional calculus allows describing and model a real object, more accurately than the classical "integer" methods, [1]. The main reason for using integer-order models was the absence of solution methods for fractional differential equations [9]. At present, there are many methods for approximation of the fractional derivative and integral [1, 10].

To encrypt the message using a complex network, for this case, it is needed to synchronize the network first. Once done, any oscillator in the network is selected. A state variable of the selected oscillator is used to encrypt the message, based on the criteria mentioned in Sec. 4. Then, the selected state variable is modulated and used to encrypt the same message to compare the results.

The modulation of chaotic signals has been applied to secure communications schemes. In [11], the authors use chaotic modulation schemes to generate chaotic symbols to improve the physical layer security. In this paper, the chaotic signals are modulated to improve the encryption quality by shifting the energy to the frequency band of the message to be encrypted.

This paper is organized as follows: Section 2 shows some notations and definitions of the fractional calculus. Section 3 shows the synchronization results of a regular complex network composed of N-coupled identical fractional order Lü chaotic oscillators. In Sec. 4, the chaotic encryption results are shown. In Sec. 5, a physical implementation is shown. Finally, in Sec. 6, the conclusions are given.

2. Preliminaries

The term of the fractional derivative was initially found in a letter written for l'Hopital by Leibniz in 1695. In it, the possibility of generalizing the operation of differentiation to non-integers was mentioned. In this section, the method used to solve the fractional order differential equations is shown.

2.1. Fractional order integrals and derivatives

One of the most popular methods for numerical solutions of the fractional-order integrals and derivatives is the Grünwald-Letnikov method. A numerical approximation can be obtained by the following expression derived from the Grünwald-Letnikov definition [1,12]:

$$_{k-L_m/h}D^q_{t_k} f(t) \approx h^{-q} \sum_{j=0}^{k} (-1)^j \left(\begin{array}{c} q \\ j \end{array} \right) f(t_{k-j}), \quad (1)$$

The Eq. (1) represents a numerical approximation to de $q-th$ derivative at points kh, where $k \in \mathbb{N}$,, $k \neq 0$ and h is the time step. The constant L_m is the "memory length" and

$$(-1)^j \left(\begin{array}{c} q \\ j \end{array} \right),$$

are the binomial coefficients $c_j^{(q)}, j \in \mathbb{N}$, calculated as follows:

$$\begin{aligned} c_0^{(q)} &= 1, \\ c_j^{(q)} &= \left(1 - \frac{1+q}{j}\right) c_{j-1}^{(q)}. \end{aligned} \quad (2)$$

A general numerical solution of the fractional-order differential equation can be obtained:

$$_aD_t^q y(t) = f(y(t), t), \quad (3)$$

The Eq. (3) can be expressed as:

$$y(t_k) = f(y(t_k), t_k) h^q - \sum_{j=v}^{k} c_j^{(q)} y(t_{k-j}). \quad (4)$$

2.2. Complex networks and synchronization

Considering a complex network composed of N identical n-dimensional dynamic subsystems. Each chaotic oscillator is defined by:

$$_0D_t^{q_\eta} x_{\eta,i}(t) = f_\eta(x_i, t) + u_{\eta,i}, \quad (5)$$

with $\eta = 1, 2, \ldots, n$ and $i = 1, 2, \ldots, N$.

The $x_{\eta,i}(t)$ and $u_{\eta,i}$ terms are the state variables and the control law respectively of the state η in the oscillator i. The control laws are defined as follows:

$$u_{\eta,i} = \delta c \sum_{j=1}^{N} a_{ij} x_j, \; i = 1, 2, \ldots, N. \quad (6)$$

The constant $c > 0$ is the coupling strength. The constant $\delta = 0$ if η is not the coupling state, $\delta = 1$ otherwise. $A = (a_{ij}) \in \mathbb{R}^{N \times N}$ is a constant matrix that denotes the connections between the oscillators in the complex network. If there exists a connection between the oscillators i and j, then the element $a_{ij} = 1$, otherwise $a_{ij} = 0$ for $i \neq j$. The diagonal elements of matrix A are calculated as follows:

$$a_{ii} = -\sum_{j=1, j\neq i}^{N} a_{ij} = -\sum_{j=1, j\neq i}^{N} a_{ji}, \; i = 1, 2, \ldots, N. \quad (7)$$

The identical synchronization of the dynamical network is achieved, if the synchronization error between the state η of the oscillators i and j is zero as $t \to \infty$, i.e. [13]:

$$\lim_{t\to\infty} \parallel x_{\eta,i}(t) - x_{\eta,j}(t) \parallel = 0, \quad (8)$$

with $i \neq j$.

The coupling strength c is calculated according to the following lemma [14]:

Lemma 1. *Consider network (5). Let λ_2 be the largest nonzero eigenvalue of the coupling matrix A of the complex network. The synchronization state of the network (8) defined by $x_1(t) = x_2(t) = \cdots = x_N(t)$ is asymptotically stable if*

$$\lambda_2 \leq -\frac{T}{c} \quad (9)$$

where $c > 0$ is the coupling strength of the network and $T > 0$ is a positive constant such that zero is an exponentially stable point of the n-dimentional system

$$\begin{aligned} \dot{y_1} &= f_1(y) - Ty_1, \\ \dot{y_2} &= f_2(y), \\ \dot{y_n} &= f_n(y). \end{aligned} \tag{10}$$

By the condition (12)*, the network achieves synchrony if λ_2 is negative enough. T is a constant such that the self-feedback term $-Ty_1$ stabilizes an isolated system.*

It is important to mention that the **Lemma 1** is not adapted to the fractional-order systems case.

3. Synchronization of N-coupled fractional-order Lü chaotic oscillators via coupling matrix

In this section, the same principles of **Lemma 1** are applied to calculate an approximate coupling strength c. This, to achieve the synchronization of a non-directed complex network composed by N identical fractional-order Lü chaotic oscillators coupled in a star topology.

3.1. Fractional-order Lü chaotic oscillator

The Lü system is known as a bridge between the Lorenz system and Chen's system [1]. Its fractional version is described as follows [15]:

$$\begin{cases} {}_0D_t^{q_1} x(t) = \sigma(y(t) - x(t)), \\ {}_0D_t^{q_2} y(t) = -x(t)z(t) + \gamma y(t), \\ {}_0D_t^{q_3} z(t) = x(t)y(t) - \beta z(t). \end{cases} \tag{11}$$

The set of Eqs. (11) exhibits chaotic behavior for parameters $\sigma = 36, \beta = 3, \gamma = 20$ and orders $q_1 = q_2 = q_3 = 0.95$ [1]. Figure 1 shows the chaotic attractor of the fractional-order Lü chaotic oscillator.

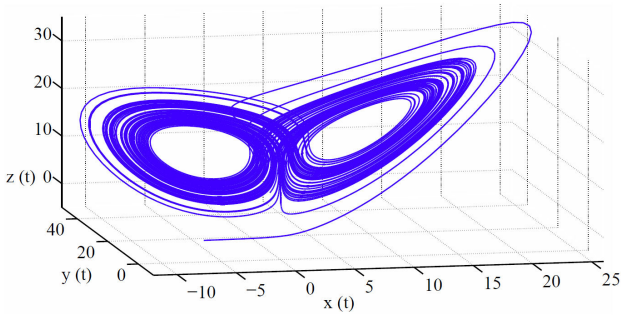

FIGURE 1. Phase space of the chaotic attractor of the Lü oscillator Eq. (12) for parameters: $\sigma = 36, \beta = 3, \gamma = 20$, and initial conditions $(x(0), y(0), z(0)) = (1, 0.1, 2.5)$ proyected onto $(x(t), y(t), z(t))$ space.

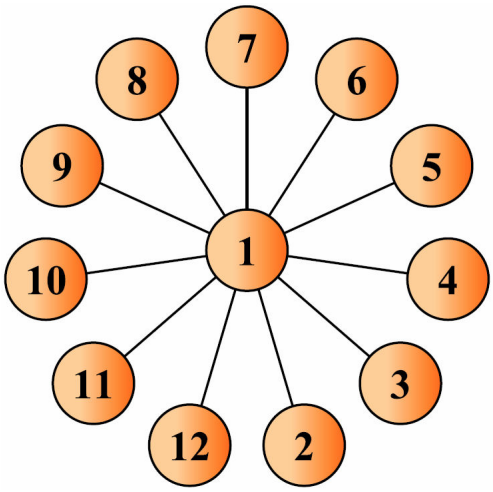

FIGURE 2. Regular star coupled network topology with bidirectional configuration.

3.2. Regular star coupled network

The following coupling matrix $A \in \mathbb{R}^{N\times N}$ $N = 12$, corresponds to the network topology shown in Fig. 2.

$$A = \begin{pmatrix} -N+1 & 1 & \cdots & 1 & 1 \\ 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & -1 & 0 \\ 1 & 0 & \cdots & 0 & -1 \end{pmatrix}. \tag{12}$$

In this case, the chaotic oscillators are coupled by the second state variable, *i.e.*, $\eta = 2$. By means of the Eq. (6), $\delta = 0$ if $\eta \neq 2$. Therefore, the control laws $u_{2,i}$ for $i = 1, \ldots, 12$ are applied to the state $y_i(t)$ of the complex network. The mathematical model of the complex network is described as follows:

$$\begin{cases} {}_0D_t^{q_1} x_i(t) = \sigma(y_i(t) - x_i(t)), \\ {}_0D_t^{q_2} y_i(t) = -x_i(t)z_i(t) + \gamma y_i(t) + u_{2,i}, \\ {}_0D_t^{q_3} z_i(t) = x_i(t)y_i(t) - \beta z_i(t), \end{cases} \tag{13}$$

where $i = 1, 2, 3, \ldots, 12$.

The control laws are defined by:

$$\begin{aligned} u_{2,1} &= c(-11y_1 + y_2 + y_3 + y_4 + y_5 + y_6 \\ &\quad + y_7 + y_8 + y_9 + y_{10} + y_{11} + y_{12}), \\ u_{2,2} &= c(y_1 - y_2), \\ &\vdots \quad \vdots \\ u_{2,12} &= c(y_1 - y_{12}). \end{aligned} \tag{14}$$

Table I shows the initial conditions of each oscillator present in the network.

TABLE I. Initial conditions of the complex network.

Oscillator	$x(0)$	$y(0)$	$z(0)$
1	5.0003	−8.3208	−2.9502
2	−1.3903	2.1136	−8.3510
3	2.3582	−6.0642	0.3310
4	3.2618	1.6353	5.4132
5	5.0304	−3.2545	1.2853
6	−4.7219	−6.6089	4.6241
7	0.0002	−0.2746	4.5556
8	2.9729	1.7510	6.2513
9	4.6489	1.1988	−3.4518
10	−3.2578	5.9605	−8.0592
11	−0.1223	−9.7442	5.1025
12	4.3086	0.0058	−0.3542

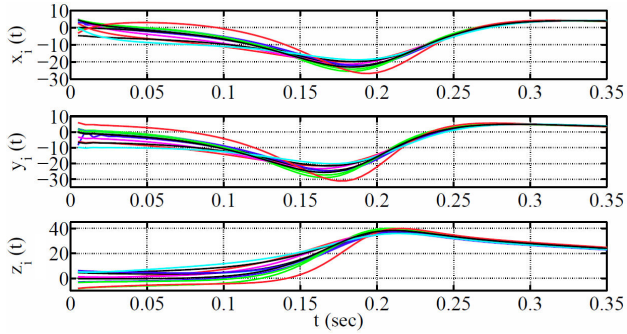

FIGURE 3. Temporal evolution of some state variables of the complex network: $x_i(t)$, $y_i(t)$, $z_i(t)$, (where $i = 1, 2, ..., 6$).

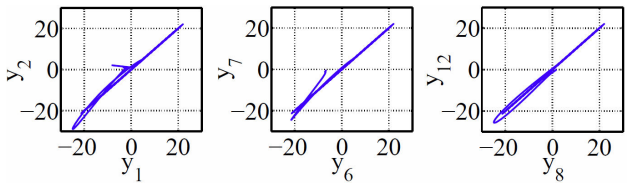

FIGURE 4. Phase portrait of some states of the complex network: y_1 vs y_2, y_6 vs y_7, y_8 vs y_{12}.

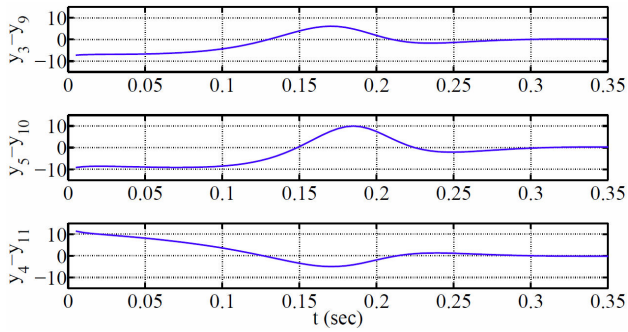

FIGURE 5. Time evolution of the synchronization error between some state variables of the complex network: $y_3 - y_9$, $y_5 - y_{10}$, $y_4 - y_{11}$.

Applying the principles of **Lemma 1**, the network achieves synchronization with an aproximate coupling strength $c = 19$. The network achieves identical synchronization and can be graphically observed in Fig. 3.

Additionally, Fig. 4 shows some phase portraits of $y_i(t)$ state variables of the network. The synchronization errors between some of the $y_i(t)$ state variables of the complex network are shown in Fig. 5.

4. Encryption process

In this section, the process to encrypt a voice message is shown. First, the message is encrypted using a selected state variable of a fractional-order Lü chaotic oscillator. Then, the state variables are modulated and used to encrypt the same message. The results are compared.

4.1. Chaotic encryption

By the conventional additive method, a chaotic signal and the message signal are added. This encrypted signal is sent through a public channel. A second chaotic signal is sent and used by the receptor to reproduce a dynamic equivalent to the chaotic signal used to encrypt the message. This signal is subtracted from the encrypted signal, and the message is restored [16]; this is illustrated in Fig. 6.

In [17], the authors select a state variable from the network in order to encrypt the message, based on the total energy provided by the chaotic signals and the frequency location of the message. It is important to mention that, once the complex network achieves synchrony, any chaotic oscillator can be selected from the network to use its state variables.

According to the previously mentioned criteria [17]:

Criterion $\mathbf{J_1}$: selection based on the chaotic signal energy

$$\sum_{n=0}^{N-1} |x_c(n)|^2 \gg \sum_{n=0}^{N-1} |m(t)|^2, \tag{15}$$

with the chaotic signal $x_c(n)$, and the message signal $m(t)$, the criterion $\mathbf{J_1}$ compares and calculate how many times the energy of $x_c(n)$ is higher than the energy of $m(t)$. If $\mathbf{J_1} \gg 1$ leads to a good encryption.

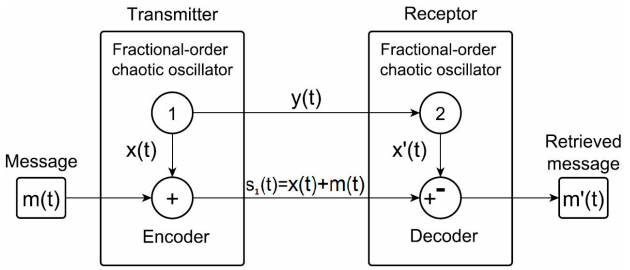

FIGURE 6. Communication scheme using the conventional additive encryption method. Message $m(t)$, encrypted message $s(t)$, and retrieved message $m'(t)$.

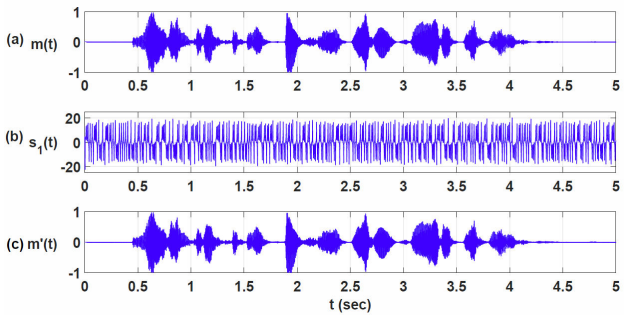

FIGURE 7. a) Message to be encrypted $m(t)$, b) Encrypted message $s_1(t)$, and c) Retrieved message $m'(t)$.

Criterion $\mathbf{J_2}$: selection based on the chaotic signal energy in the frequency domain

$$\sum_{k=0}^{N-1} \mu(k)|X_c(k)|^2 \gg \sum_{k=0}^{N-1} \mu(k)|X_m(k)|^2, \qquad (16)$$

with the chaotic sampled signal $X_c(k)$, the message sampled signal $X_m(k)$, and $\mu(k)$ the frequency weighting function. The criterion $\mathbf{J_2}$, based on the frequency band of the message, shows how many times the energy of the weighted signal $X_c(k)$ is higher than the energy of the weighted signal $X_m(k)$. If $\mathbf{J_2} \gg 1$ leads to good encryption in the selected frequency band.

For numerical solutions, a discrete time criterion is used due to the integration step. The Fast Fourier Transform is used in order to transform the signals from time domain to a frequency domain.

Table II shows the resilts of the criteria $\mathbf{J_1}$ and $\mathbf{J_2}$ in numerical values. The message to be encrypted: "data encrypted with fractional-order chaotic oscillators", is a voice message located in a frequency band of 0.3 kHz - 3 kHz [3] recorded with a sampling frequency $F_s = 11.025$ kHz.

From Table II, by the $\mathbf{J_1}$ criterion: $z(t)$ provides the highest value. The $y(t)$ state is needed to achieve synchrony. In order to retrieve the message, $y(t)$ is sent via a public channel. We consider $x(t)$ and $z(t)$ as the only possible candidates to encrypt the message. The $z(t)$ state provides the highest energy value in the frequency band in which our message is located. However, we have selected the $x(t)$ state to encrypt the message in order to compare the results obtained after the state variables modulation. Hence, it is selected as the state variable to encrypt the message; the additive chaotic encryption is used.

TABLE II. Criteria values for the chaotic signals of the synchronization of the complex network.

State	$E_c(10^7)$	$\mathbf{J_1}(10^4)$	$\mathbf{J_2}$
$x(t)$	0.2943	0.2406	26.5344
$y(t)$	0.3172	0.2593	44.1517
$z(t)$	1.9887	1.6257	35.6678

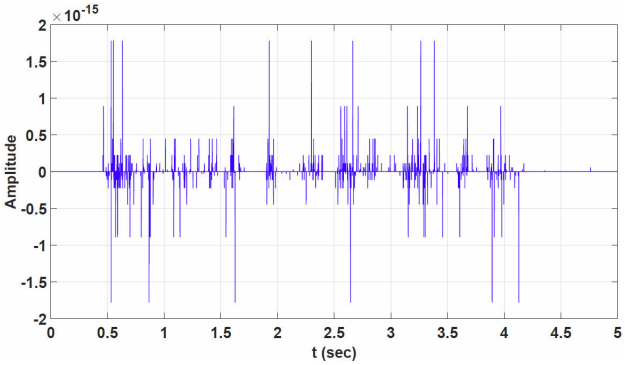

FIGURE 8. Time evolution of the error between the message $m(t)$ and the retrieved message $m'(t)$.

The encryption results are shown in Fig. 7. Where (a) $m(t)$, is the message to encrypt, (b) $s_1(t) = x(t) + m(t)$, is the encrypted message, and (c) $m'(t) = s_1(t) - x'(t)$, represents the retrieved message. In Fig. 8, the error between the message $m(t)$ and the retrieved message $m'(t)$ is shown.

4.2. Modulation of the fractional-order Lü chaotic oscillator state variables

In this section, the chaotic state variables are modulated and located in the frequency band of the message as an alternative way to ensure that the highest possible energy values provided by the chaotic signals are utilized. The above, leads to an encryption quality improvement.

The resulting product of a sequence $x(n)$ and $e^{j\omega_0 n}$ is equal to a frequency translation of the spectrum $X(\omega)$ by ω_0 [4]. The state variables modulation of the first chaotic oscillator of the previously synchronized network is performed as follows:

$$\begin{aligned} x_{f_0}(n) &= x_1(n)\cos(\omega_0 n), \\ y_{f_0}(n) &= y_1(n)\cos(\omega_0 n), \\ z_{f_0}(n) &= z_1(n)\cos(\omega_0 n), \end{aligned} \qquad (17)$$

where $\omega_0 = (2\pi f_0/F_s)$. The chaotic signal is shifted to the frecuency band f_0. Considering the message $m(t)$ used in Subsec. 4.1: $\omega_0 = \pi(300 \text{ Hz}/5512.5 \text{ Hz})$. The communication scheme applying the state variables modulation is shown in Fig. 9.

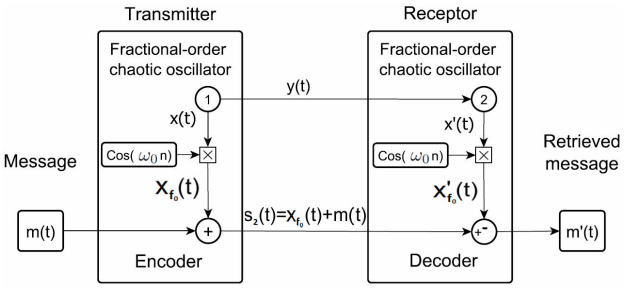

FIGURE 9. Communication scheme using the conventional additive encryption method and $x(t)$ state variables modulation.

In Table III, $\mathbf{J_2}$ represents the total amount of energy provided by the chaotic signal at the frequency band of the message. $\mathbf{J_{2m}}$ represents the total amount of energy provided by the chaotic signal at the frecuency band of the message after the state variable modulation. The constant B represents a relation between $\mathbf{J_{2m}}$ compared with $\mathbf{J_2}$.

It is important to mention that the energy values do not increase by a gain application. The increase of energy values shown in this paper is the result of correctly locating the chaotic signals to the frequency band of the message.

As previously mentioned, the second state of the chaotic oscillator, in this case $y_{f_0}(t)$, is the coupling state variable. It is needed to achieve synchrony and therefore, it is unavaiable to be selected as a candidate to encrypt the message.

From Table III, it is observed that $x_{f_0}(t)$, employing criterion $\mathbf{J_{2m}}$, provides the highest energy value at the frecuency band in which the message is located. Therefore, $x(t)$ is selected to encrypt the message.

TABLE III. Criteria values for the chaotic signals of the synchronization of the complex network.

State	$\mathbf{J_2}$	$\mathbf{J_{2m}}$	B
$x_{f_0}(t)$	26.5344	957.1	36.1
$y_{f_0}(t)$	44.1517	1019.6	23.1
$z_{f_0}(t)$	35.6678	713.6	20

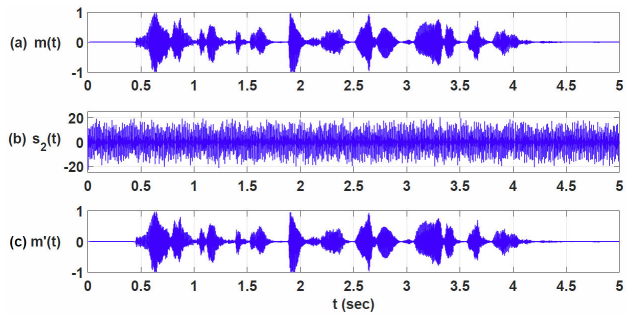

FIGURE 10. a) Message to be encrypted $m(t)$, b) Encrypted message $s_2(t)$, and c) Retrieved message $m'(t)$.

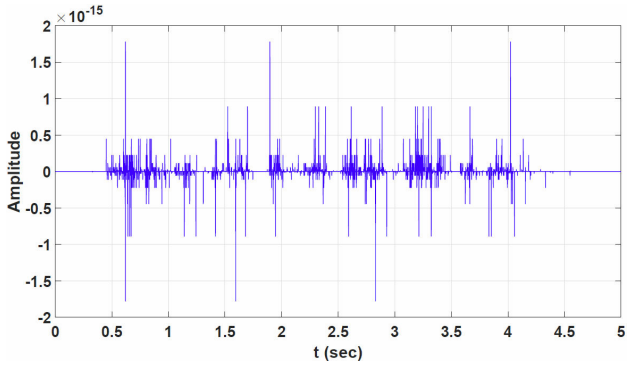

FIGURE 11. Time evolution of the error between the message $m(t)$ and the retrieved message $m'(t)$ after modulating $x(t)$.

Figure 10 shows the encryption results are after the state variables modulation. Where (a) $m(t)$, is the message to encrypt, (b) $s_2(t) = x_{f_0}(t) + m(t)$, is the encrypted message, and (c) $m'(t) = s_2(t) - x'_{f_0}(t)$, represents the retrieved message.

Figure 11 shows the error between the message $m(t)$ and the retrieved message $m'(t)$ when $x_{f_0}(t)$ is used.

5. Physical implementation

In this section, FPGA realization of a communication scheme composed of two identical fractional-order systems is presented.

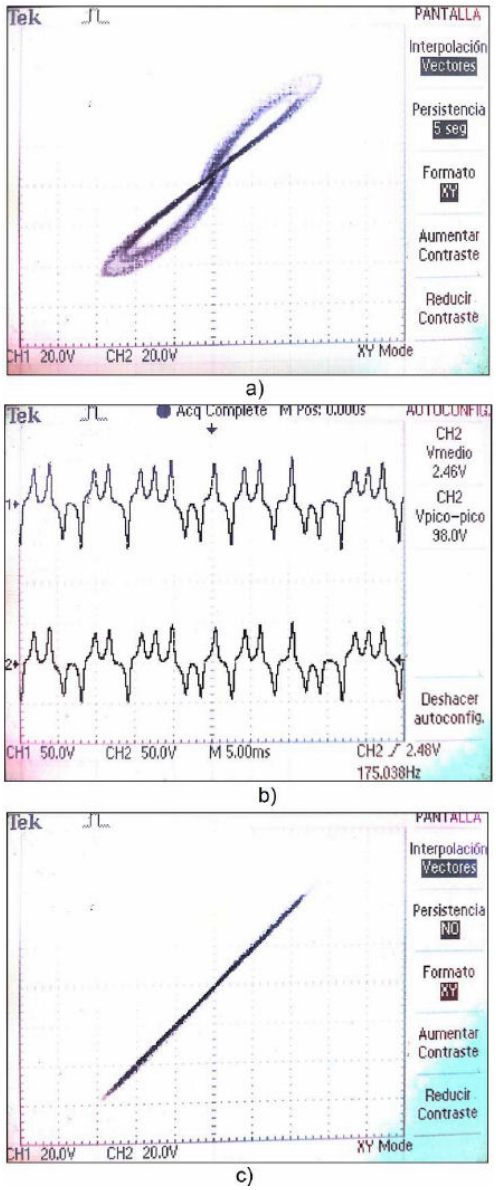

FIGURE 12. a) $2D$ chaotic strange attractor formed by $x[t_k]$ vs $y[t_k]$, b) Time evolution of $x[t_k]$ and $y[t_k]$, c) Confirmed synchronization of the second state $y[t_k]$ vs $y'[t_k]$.

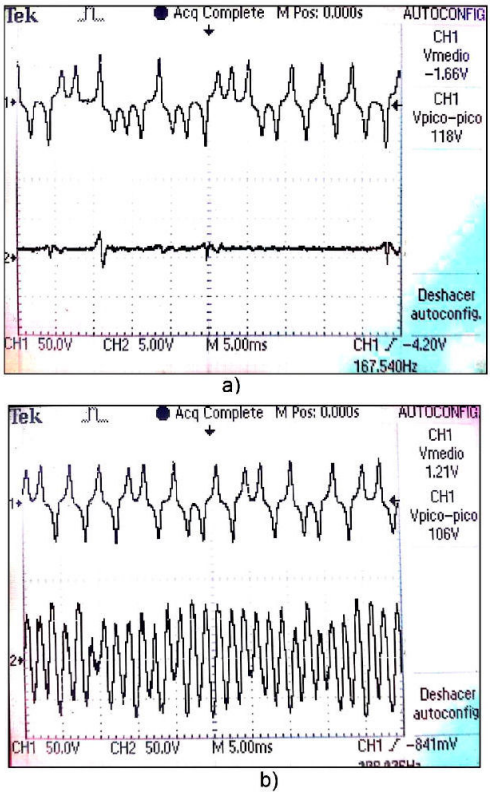

FIGURE 13. a) Time evolution of the state variable $y[t_k]$ (above) and the time evolution of the synchronization error $e[t_k] = y'[t_k] - y[t_k]$ (under), b) Dynamic of the state variable $y[t_k]$, and the encrypted data signal $s[t_k] = x[t_k] + m[t_k]$.

We use two National Instruments MyRIO 1900 for implementation. Both MyRIO are connected following a transmitter-receiver scheme. Their technical characteristics are identical and they are described as follows:

- Xilinx Z-7010 processor 667 MHz (ARM Cortex A9 $\times 2$ cores 28mm process NEON SIMD, VFPv3 Vector Float). Memory: NV: 256 MB, DDR3 512 MB, 533 MHz, 16 bits. FPGA type: same as the processor. Wireless: IEEE 802.11 b, g, n ISM 2.4 GHz 20 MHZ. USB 2.0 Hi-Speed, breakout board support, 2 ports of 16 Digital I/O lines, 3 axis accelerometer. Max power consumption: 14 W, typical idle: 2.6 W and LED's.

By using the Grundwald-Letnikov method to solve the fractional order numerical integration, the Lü digital aproximated system is defined as:

$$\begin{cases} x_i[t_{k+1}] = (\sigma(y_i[t_k] - x_i[t_k])h^{q_1} - Q_1, \\ y_i[t_{k+1}] = (-x_i[t_k]z_i[t_k] + \gamma y_i[t_k] + u_{2,i})h^{q_2} - Q_2, \\ z_i[t_{k+1}] = (x_i[t_k]y_i[t_k] - \beta z_i[t_k])h^{q_3} - Q_3. \end{cases} \tag{18}$$

Where

$$Q_1 = \sum_{j=0}^{L_m-1} c_j^{q_1} x_i[t_k - j],$$

$$Q_2 = \sum_{j=0}^{L_m-1} c_j^{q_2} y_i[t_k - j]$$

and

$$Q_3 = \sum_{j=0}^{L_m-1} c_j^{q_3} z_i[t_k - j].$$

Due to hardware storage capacity limitations, we use a simple master-slave topology and a memory length $L_m = 8$. The parameters previously shown in the subsection 3.1 are used.

Consider the encoder modulated states defined by $x[t_k]$, $y[t_k]$, $z[t_k]$, and the decoder modulated states defined by $x'[t_k]$, $y'[t_k]$, $z'[t_k]$.

Figure 12a) shows the $2D$ atractor $x[t_k]$ vs $y[t_k]$. Figure 12b) shows $x[t_k]$ (above) and $y[t_k]$ (under) time evolution. Figure 12c) shows $y[t_k]$ vs $y'[t_k]$ portrait, providing a graphical demonstration of synchrony.

Figure 13a) shows $y[t_k]$ time evolution (above) and the synchronization error defined by $e[t_k] = y'[t_k] - y[t_k]$ (under). Figure 13b) shows $y[t_k]$ (above) and the encrypted data defined by $s[t_k] = x[t_k] + m[t_k]$ (under).

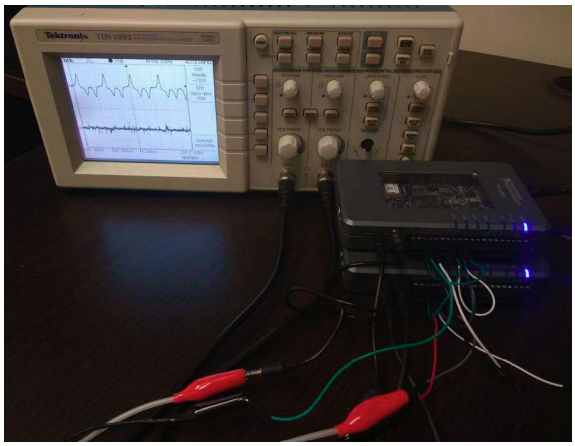

FIGURE 14. Photograph of the hardware used for physical implementation.

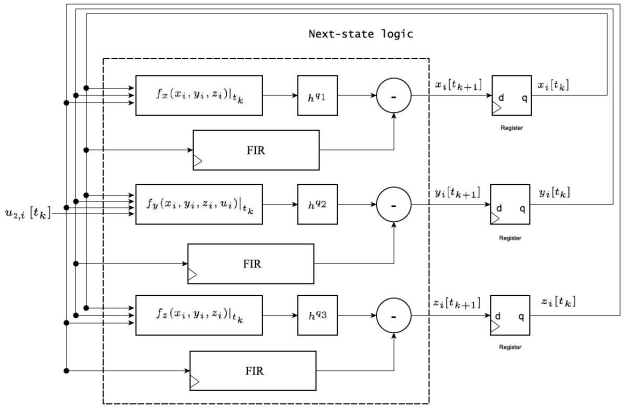

FIGURE 15. Block diagram of the proposed implementation of the oscillator i. The next state logic for each state register is calculated by Q_1, Q_2, and Q_3.

Figure 14 shows the hardware used for physical implementation.

Figure 15 shows the block diagram corresponding to (22). We use a memory length $L_m = 8$ in order to save resources of the FPGA. The FIR blocks correspond to the filtering process of the states through the binomial coefficients

6. Conclusions

To retrieve the message, $y(t)$ is used to achieve synchronization. Thereby, $y(t)$ is not eligible as a candidate to encrypt the message. We only consider $x(t)$ and $z(t)$ as candidates to encrypt the message. Providing the highest value of energy is not enough property to select a signal as a good candidate to encrypt a message. Considering the frequency band in which the message is located is recommended. The $\mathbf{J_2}$ values show how $z(t)$ provides the highest energy value. However, using the criterion $\mathbf{J_{2m}}$, we can observe that the energy of $x_{f_0}(t)$ is higher than the energy provided by $z_{f_0}(t)$. By modulating the fractional order Lü chaotic oscillator state variables, we shifted the energy to the frequency band of the message, helping us to improve the encryption quality by an approximate factor of 36.

Acknowledgements

This work was supported by CONACYT México under Research Grant No. 166654, $\mathrm{A1}-5-31628$ and by "Facultad de Ingeniería Mecánica y Eléctrica"(FIME-UANL).

1. I. Petráš, *Fractional-Order Nonlinear Systems* (Springer-Verlag, Berlin, 2011), https://doi.org/10.1007/978-3-642-18101-6.
2. H. G. Schuster and W. Just, *Deterministic Chaos*, 4th ed. (Wiley-VCH, Weinheim, 2005), https://doi.org/10.1002/3527604804.
3. W. Tomasi, *Electronic Communication Systems*, 4th ed. (Prentice Hall, New Jersey, 2001).
4. J. G. Proakis and D. K. Manolakis, *Digital Signal Processing*, 4th ed. (Prentice Hall, New Jersey, 2007).
5. L. M. Pecora and T. L. Carroll, Synchronization in chaotic systems, *Phys. Rev. Lett.* **64** (1990) 821, https://doi.org/10.1103/PhysRevLett.64.821.
6. O. I. Moskalenko, A. A. Koronovskii, and A. E. Hramov, Generalized synchronization of chaos for secure communication: Remarkable stability to noise, *Phys. Lett. A* **374** (2010) 2925, https://doi.org/10.1016/j.physleta.2010.05.024.
7. A. D. Pano-Azucena, B. Ovilla-Martinez, E. Tlelo-Cuautle, J. M. Muñoz-Pacheco, and L. G. de la Fraga, FPGA-based implementation of different families of fractional-order chaotic oscillators applying Grünwald-Letnikov method, *Commun. Nonlinear Sci. Numer. Simul.* **72** (2019) 516, https://doi.org/10.1016/j.cnsns.2019.01.014.
8. A. Bayani, M. A. Jafari, K. Rajagopal, H. Jiang, and S. Jafari, A novel fractional-order chaotic system with specific topology: from proposing to FPGA implementation, *Eur. Phys. J. Spec. Top.* **226** (2017) 3729, https://doi.org/10.1140/epjst/e2018-00031-y.
9. I. Podlubny, I. Petráš, B. M. Vinagre, P. O'Leary, and L'. Dorčák, Analogue Realizations of Fractional-Order Controllers, *Nonlinear Dyn.* **29** (2002) 281, https://doi.org/10.1023/A:1016556604320.
10. C. P. Li and Z. G. Zhao, Introduction to fractional integrability and differentiability, *Eur. Phys. J. Spec. Top.* **193** (2011) 5, https://doi.org/10.1140/epjst/e2011-01378-2.
11. C. Seneviratne and H. Leung, Mixing chaos modulations for secure communications in OFDM systems, *Eur. Phys. J. Spec. Top.* **226** (2017) 3287, https://doi.org/10.1140/epjst/e2016-60352-5.
12. I. Podlubny, *Fractional differential equations* (Academic Press, San Diego, 1999).
13. S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares, and C. S. Zhou, *Phys. Rep.* **366** (2002) 1, https://doi.org/10.1016/S0370-1573(02)00137-0.
14. X. F. Wang and G. Chen, Synchronization in small-world dynamical networks, *Int. J. Bifurc. Chaos* **12** (2002) 187, https://doi.org/10.1142/S0218127402004292.
15. W. H. Deng and C. P. Li, Chaos synchronization of the fractional Lü system, *Physica A* **353** (2005) 61, https://doi.org/10.1016/j.physa.2005.01.021.
16. F. Dachselt and W. Schwarz, Chaos and cryptography, IEEE Trans. *Circuits Syst. I* **48** (2001) 1498, https://doi.org/10.1109/TCSI.2001.972857.
17. A. G. Soriano-Sánchez, C. Posadas-Castillo, M. A. Platas-Garza, and D. A. Diaz-Romero, Performance improvement of chaotic encryption via energy and frequency location criteria, *Math. Comput. Simul.* **112** (2015) 14, https://doi.org/10.1016/j.matcom.2015.01.007.