Memorias del Congreso Nacional de Control Automático
ISSN: 2594-2492

Contraction-Based Chaotic Fractional-Order System Synchronization for Message Encryption ⋆

González-Olvera, Marcos A. * **Tang, Yu** **

* *Universidad Autónoma de la Ciudad de México, Colegio de Ciencia y Tecnología. Ciudad de México, México (marcos.angel.gonzalez@uacm.edu.mx)*
** *Unidad de Alta Tecnología, Facultad de Ingeniería, Universidad Nacional Autónoma de México, Juriquilla, Qro. (tang@unam.mx)*

Abstract: In this work it is presented a contraction analysis-based design for the synchronization of a pair of chaotic fractional order systems is presented. It allows to send encrypted information through a channel, using the chaotic sequence generated by a master system as a carrier signal to the second slave system which decrypts the message using a key signal. Contraction analysis gives a straightforward analysis design, one given for the synchronization and convergence of neighbor trajectories of both systems. Numeric examples are presented to show the effectiveness of the proposed design.

Keywords: Fractional order systems, adaptive observers.

1. INTRODUCTION

Even though the concept of integro-differential fractional equations were first proposed at the end of the 17th century and taken into account as a research subject until 1884, their application to describe dynamic systems has only been gaining attention in recent years due to the fact that several classes of physical systems, especially those including diffusion dynamics or friction, as well as memory and hereditary properties in materials and systems can be better and more succinctly described by fractional derivatives and integrals, rather than by their integer counterparts [Caponetto, 2010]. As usually the integer integral or derivative is represented by the operators J^n and D^m respectively, where $n \in \mathbb{N}$; so, fractional integral and derivative are typically described also as the operators J^β and D^α, where $\alpha, \beta \in \Re$.

As the same tools used to analyse linear systems with integer differentials and integrals, such as the Laplace transform and the Fourier analysis can be extrapolated and used in linear fractional ones, some methods have been proposed to approximate the solution given by a fractional differential equation of fractional differential system (FOS), from a higher-order transfer function with integer derivatives [Mansouri et al., 2010, Oustaloup et al., 2000] to the analysis of the step response [Dorcák et al., 2002], similar to the case of first and second-order systems. In most cases the parameters of FOSs are assumed known or obtained from a physical analysis of the system, especially regarding the fractional α and β.

New techniques for analysis of linear and nonlinear fractional-order systems have been proposed in recent years. Lyapunov analysis for stability has been extended to the fractional case [Aguila-Camacho et al., 2014, Duarte-Mermoud et al., 2015], as well as for the Barbalat lemma [Navarro-Guerrero and Tang, 2017], that have been used to propose a contraction-analysis approach to not only the convergence of the trajectories of a FOS to a fixed point, but also convergence among trajectories based on contraction-analysis [González-Olvera and Tang, 2018]. This approach has been proven to be useful in analysis and design of synchronization schemes for chaotic systems, investigated [Zhu et al., 2009] to study its applications [Angulo-guzman et al., 2016, Delgado and Duarte, 2014, Hartley et al., 1995] and to design secure communications [Kiani-B et al., 2009].

In this work we present an observer of a synchronization scheme for a chaotic fractional-order systems in order to send an encrypted message, based on contraction theory analysis and design. The paper is organized as follows: In Section 2, a brief description of fractional calculus and systems are given and the problem statement is given. In Section 3, the algorithm for the synchronization scheme based on contraction theory is presented, and in Section 4 results are shown in order to illustrate the effectiveness of the method. Finally, conclusions are discussed in Section 5.

2. BACKGROUND

From a mathematical point of view, a fractional order integral or derivative is defined as an extrapolation of the definition of the integer-order integral or derivative of a certain function $f(t)$, seen as a general fractional differential operator D^α. In this work we use the *Caputo Fractional Differential Operator* [Caputo, 1967]:

$$ {}_a^{\mathcal{C}}D_t^\alpha f(t) = f^{(\alpha)}(t) = $$

⋆ Author wants to thank UACM for its support to this work

$$\begin{cases} \dfrac{1}{\Gamma(n-\alpha)} \displaystyle\int_a^t \frac{\frac{d^n f(\tau)}{dt^n}}{(t-\tau)^{\alpha+1-n}} d\tau, \in (n-1,n), & n \in \mathbb{N} \\ \dfrac{d^n}{dt^n} f(t), & \alpha = n \in \mathbb{N}. \end{cases} \tag{1}$$

as in the area of control systems, generally the Caputo's definition is preferred, since the initial conditions typically associated with physical interpretation are involved, such as the integer derivative at $t = 0$. In this work we use the simplified notation ${}_0^C D_t^\alpha f(t) = D^{(\alpha)} = f^{(\alpha)}(t)$.

2.1 Contraction analysis for fractional-order nonlinear systems and asymptotic convergence

Let a fractional-order state space system with an initial condition be defined by the fractional differential equation

$$\mathbf{x}^{(\alpha)}(t) = \mathbf{f}(\mathbf{x}(t), t),\ \mathbf{x}(t_0) = \mathbf{x}_0, \tag{2}$$

where $\mathbf{x}(t) \in \Re^n$ is the state vector, $t \geq t_0 = 0$, $\mathbf{f} : \Re^n \times \Re^+ \to \Re^n$ a nonlinear continuously differentiable vector field, and $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_n]^T$ are the fractional orders $\alpha_i \in (0, 1]$. This definition includes systems with external inputs $\mathbf{f}(\mathbf{x}(t), t) = \bar{\mathbf{f}}(\mathbf{x}(t), \mathbf{u}(t), t)$ or with a feedback control $\mathbf{u}(t) = \mathbf{u}(\mathbf{x}(t), t)$.

Assumption 1. (2) is of *commensurate order*, so α is taken as a single scalar, where $0 < \alpha \leq 1$.

Consider then a given trajectory $\mathbf{x}(t)$ of the system (2), (and with little abuse of notation (let $\mathbf{x} = \mathbf{x}(t)$ when possible) and in a *fixed time* an adjacent trajectory $\tilde{\mathbf{x}}(t)$ defined as $\tilde{\mathbf{x}}(t) = \mathbf{x}(t) + \delta\mathbf{x}(t)$, where $\delta\mathbf{x}(t)$ is the *virtual displacement* from the original trajectory. Then $\|\delta\mathbf{x}(t)\|$ as the differential distance between them at a fixed time. Given that the fractional derivative is a linear operator, the dynamics of $\tilde{\mathbf{x}}(t)$ is described by:

$$\begin{aligned} D^\alpha \tilde{\mathbf{x}}(t) &= D^\alpha \left(\mathbf{x}(t) + \delta\mathbf{x}(t)\right) \\ &= D^\alpha \mathbf{x}(t) + D^\alpha \delta\mathbf{x}(t) = \mathbf{f}(\mathbf{x}(t), t) + \delta\mathbf{x}^{(\alpha)}(t), \end{aligned} \tag{3}$$

The dynamics of the virtual displacement of each $x_i^{(\alpha)}(t) = f_i(\mathbf{x}(t), t)$ at a fixed time is given by

$$\delta[x_i^{(\alpha)}(t)] = \delta[f_i(\mathbf{x}(t), t)] = \delta[f_i(x_1, \ldots, x_n, t)] = \tag{4}$$

$$\sum_{k=1}^{n} \left(\frac{\partial f_i}{\partial x_i}\right)(\mathbf{x}(t), t)\delta x_k(t). \tag{5}$$

Therefore, as $\delta[D^\alpha x_i(t)] = D[\delta x_i^{(\alpha)}(t)] = \delta x_i^{(\alpha)}(t)$ *at a fixed time* t, we get

$$\delta\mathbf{x}^{(\alpha)} = \frac{\partial \mathbf{f}}{\partial \mathbf{x}}\delta\mathbf{x} \triangleq J(\mathbf{x}, t)\delta\mathbf{x}, \tag{6}$$

where $J(\mathbf{x}, t) = [\partial f_i(\mathbf{x}(t), t)/\partial x_j(t)] = \partial\mathbf{f}/\partial\mathbf{x}$, that is, the jacobian matrix of $\mathbf{f}(\mathbf{x}(t), t)$. It is interesting to note how, given that the virtual displacement is given in a *fixed time*, no fractional derivatives appear at the right side of (6).

As consequence, for adjacent trajectories of (2), the dynamics of their difference is given by (6), that depends on the properties of $J(\mathbf{x}, t)$, where its symmetric part is

$$J_s = \frac{1}{2}\left(J(\mathbf{x}, t) + J^T(\mathbf{x}, t)\right),$$

and $\bar{\lambda}_m = \sup_{x\in\mathcal{X}}\{\lambda_m(\mathbf{x}(t), t)\}$ the bound of its largest eigenvalue in a given region of the state-space $\mathbf{x} \in \mathcal{X} \subseteq \Re^n$.

Let the Euclidian distance be given by $V(\delta\mathbf{x}(t)) = \frac{1}{2}\|\delta\mathbf{x}(t)\|^2 = \frac{1}{2}\delta\mathbf{x}^T(t)\delta\mathbf{x}(t)$. Using the result given by Águila-Camacho et al. [2014], its fractional derivative $D^\alpha V(\delta\mathbf{x}(t))$ results in the inequality:

$$\begin{aligned} D^\alpha V(\delta\mathbf{x}(t)) &\leq \delta\mathbf{x}^T(t) D^\alpha \delta\mathbf{x}(t) = \delta\mathbf{x}^T(t) J(\mathbf{x}(t), t)\delta\mathbf{x}(t) \\ &\leq \bar{\lambda}_m \delta\mathbf{x}^T(t)\delta\mathbf{x}(t). \end{aligned}$$

So we have the fractional-order differential inequality

$$D^\alpha V(\delta\mathbf{x}(t)) \leq 2\bar{\lambda}_m V(\delta\mathbf{x}(t)). \tag{7}$$

Therefore, there must be a non-negative function $m(t)$ such that the equality is met, *i.e.*

$$D^\alpha V(\delta\mathbf{x}(t)) = 2\bar{\lambda}_m V(\delta\mathbf{x}(t)) - m(t). \tag{8}$$

Given that $0 < \alpha \leq 1$, let $\mathcal{L}\{V(\delta\mathbf{x}(t))\} \triangleq V(\delta\mathbf{x}(s))$ and $\mathcal{L}\{m(t)\} \triangleq M(s)$, from (8) we obtain:

$$\begin{aligned} \mathcal{L}\{D^\alpha V(\delta\mathbf{x}(t))\} &= s^\alpha V(\delta\mathbf{x}(s)) - s^{\alpha-1}V(\delta\mathbf{x}(0)) \\ &= 2\bar{\lambda}_m V(\delta\mathbf{x}(s)) - M(s), \end{aligned}$$

so

$$V(\delta\mathbf{x}(s))(s^\alpha - 2\bar{\lambda}_m) = s^{\alpha-1}V(\delta\mathbf{x}(0)) - M(s). \tag{9}$$

Therefore,

$$V(\delta\mathbf{x}(s)) = \frac{s^{\alpha-1}}{s^\alpha - 2\bar{\lambda}_m}V(\delta\mathbf{x}(0)) - \frac{1}{s^\alpha - 2\bar{\lambda}_m}M(s), \tag{10}$$

As for a pair of functions $g(t)$, $h(t)$ we have that the Laplace transform of its convolution is

$$\mathcal{L}\left\{\int_0^t g(t)h(t-\tau)d\tau\right\} = \mathcal{L}\{g(t) * h(t)\} = G(s)H(s).$$

We then obtain the solution in the time domain:

$$\begin{aligned} V(\delta\mathbf{x}(t)) = E_\alpha(2\bar{\lambda}_m t^\alpha)V(\delta\mathbf{x}(0)) - \\ \left(t^{\alpha-1}E_{\alpha,\alpha}(2\bar{\lambda}_m t^\alpha)\right) * (m(t)). \end{aligned} \tag{11}$$

Given that $m(t)$ and $t^{\alpha-1}E_{\alpha,\alpha}(2\bar{\lambda}_m t^\alpha)$ are non-negative functions [Li et al., 2009], then the solution to the inequality (7) is:

$$V(\delta\mathbf{x}(t)) \leq V(\delta\mathbf{x}(0))E_\alpha(2\bar{\lambda}_m t^\alpha). \tag{12}$$

Now, if in the region $\bar{\lambda}_m < 0\ \forall\ \mathbf{x} \in \mathcal{X}$, then it is guaranteed that $\lim_{t\to\infty} V(\delta\mathbf{x}) = 0$. Consequently, as $V(\delta\mathbf{x}(t)) = \frac{1}{2}\|\delta\mathbf{x}(t)\|^2$, the distance between adjacent trajectories decays inside the region as

$$\|\delta\mathbf{x}(t)\| \leq \|\delta\mathbf{x}(0)\|\sqrt{E_\alpha(2\bar{\lambda}_m t^\alpha)}, \tag{13}$$

while the states remain in the region. Therefore, it follows that $\lim_{t\to\infty}\delta\mathbf{x} = 0$ whenever $\mathbf{x}_0 \in \mathcal{X}$, and a asymptotic convergence is guaranteed.

With this result, we can give the following definition:

Definition 1. [González-Olvera and Tang, 2018] Given (2), a region $\mathcal{X}$ of the state space is called a *contractive region* if the symmetric part of the Jacobian matrix $\partial\mathbf{f}/\partial\mathbf{x}$ is negative definite for $\mathbf{x} \in \mathcal{X}$. If it is only negative semi-definite, then the region is called *semi-contractive*.

Therefore, in a contractive region the trajectories converge to each other with a distance bounded by a Mittag-Leffler vanishing function, and we can give the following theorem:

Theorem 1. [González-Olvera and Tang, 2018] If the system (2) is contractive in a given region $\mathcal{X} \subseteq \Re^n$, then if a given trajectory remains inside the region, then any nearby trajectory that starts in a ball around that trajectory converges asymptotically to the former, and the distance between them is bounded by a Mittag-Leffler vanishing function.

Now consider a different metric, seen as a change of coordinates given a linear time-invariant invertible transformation $T \in \Re^{n\times n}$ in the form

$$\delta\mathbf{z} = T\delta\mathbf{x}, \tag{14}$$

and let the generalized Jacobian matrix be defined as

$$\mathbf{F}(\mathbf{x},t) = T\frac{\partial \mathbf{f}}{\partial \mathbf{x}}T^{-1} \tag{15}$$

In this sense, a given Euclidian metric is defined for the virtual infinitesimal displacement by $||\delta\mathbf{x}||_P^2 = ||\delta\mathbf{z}||^2 = \delta\mathbf{x}^T P\delta\mathbf{x}$, with $P = T^T T$. The objective now is to analyze convergence of the trajectories of (2) and, for that matter, we can give the next definition:

Definition 2. Given (2), a region $\mathcal{X}$ of the state space is called a *contractive region* with respect to a constant uniformly positive definite metric $P = T^T T$ if there exists a positive scalar $\beta_F > 0$ such that the generalized Jacobian matrix (15) complies with $\mathbf{F}(\mathbf{x},t) \leq -\beta_F I$, or equivalently $\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right)^T P + P\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right) \leq -2\beta_F P$, for $\mathbf{x} \in \mathcal{X}$. In other words, a *contractive region* is such where the symmetric part of (15) is negative definite, while if it is only negative semidefinite, then the region is called a *semi-contractive region.*

Then we can postulate the following Theorem:

Theorem 2. If the system (2) is contractive under a given metric $P > 0$ in a given region $\mathcal{X} \subseteq \Re^n$, then adjacent trajectories inside the region converge asymptotically to each other, and their distance is bounded by a Mittag-Leffler vanishing function.

In the case of a semi-contractive region, that is, when (15) is only negative semi-definite, it can only be proven that the distance among trajectories remains bounded. Consider then the class of systems (2) that, given a diffeomorphism $\xi = (\xi_1^T, \xi_2^T)^T = \Phi(\mathbf{x})$ are transformed into

$$D^\alpha \begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix} = \begin{pmatrix}\mathbf{f}_1(\xi_1,\xi_2)\\ \mathbf{f}_2(\xi_1,\xi_2)\end{pmatrix}, \tag{16}$$

where the first variation is

$$D^\alpha \begin{pmatrix}\delta\xi_1\\ \delta\xi_2\end{pmatrix} = \begin{pmatrix}\frac{\partial \mathbf{f}_1(\xi_1,\xi_2)}{\partial \xi_1} & \frac{\partial \mathbf{f}_1(\xi_1,\xi_2)}{\partial \xi_2}\\ \frac{\partial \mathbf{f}_2(\xi_1,\xi_2)}{\partial \xi_1} & \frac{\partial \mathbf{f}_2(\xi_1,\xi_2)}{\partial \xi_2}\end{pmatrix}\begin{pmatrix}\delta\xi_1\\ \delta\xi_2\end{pmatrix}, \tag{17}$$

and consider that if $\frac{\partial \mathbf{f}_1(\xi_1,\xi_2)}{\partial \xi_2} = -\frac{\partial \mathbf{f}_2(\xi_1,\xi_2)}{\partial \xi_1}$ and $\frac{\partial \mathbf{f}_2(\xi_1,\xi_2)}{\partial \xi_2} = 0\ \forall t \geq 0$, given the positive definite function

$$V(\delta\xi_1,\delta\xi_2) = \frac{1}{2}\delta\xi_1^T\delta\xi_1 + \frac{1}{2}\delta\xi_2^T\delta\xi_2, \tag{18}$$

we have that its fractional derivative along the system trajectories complies with

$$V^{(\alpha)}(\delta\xi_1,\delta\xi_2) \leq \delta\xi_1^T\frac{\partial \mathbf{f}_1(\xi_1,\xi_2)}{\partial \xi_1}\delta\xi_1. \tag{19}$$

Therefore, we can state the following Theorem:

Theorem 3. If the system (2) is semi-contractive under the metric $P > 0$ in a given region $\mathcal{X} \subseteq \Re^n$, and if there exists some diffeomorphism $\xi = (\xi_1^T, \xi_2^T)^T = \Phi(\mathbf{x})$ such that $\frac{\partial \mathbf{f}_1(\xi_1,\xi_2)}{\partial \xi_2} = -\frac{\partial \mathbf{f}_2(\xi_1,\xi_2)}{\partial \xi_1}$, $\frac{\partial \mathbf{f}_2(\xi_1,\xi_2)}{\partial \xi_2} = 0$, and $\frac{\partial \mathbf{f}_1(\xi_1,\xi_2)}{\partial \xi_1} < 0$ for $\mathbf{x} \in \mathcal{X}$, then $\delta\xi_1 \to 0$ as $t \to 0$ with a Mittag-Leffler vanishing function, and $||\delta\xi_2||$ remains bounded.

2.2 Partial contraction

One particularly useful result of contraction analysis is that it gives analysis and design tools to determine when the trajectories of two systems will converge asymptotically, and not necessarily to an equilibrium point. That is, if the trajectories of a given system Σ_1 are a particular solution of a second system Σ_2, and it results that the latter is contractive, then its trajectories would asymptotically converge to the former.

For example, consider the pair of the scalar systems with $\alpha \in (0,1]$ $\Sigma_1 :\ y^{(\alpha)}(t) = -y(t) - y^3(t) + \sin(t) = f(y,y,t)$ and $\Sigma_2 :\ \upsilon^{(\alpha)}(t) = -\upsilon(t) - y^3(t) + \sin(t) = f(y,\upsilon,t)$. When $\upsilon = y$, the trajectories of Σ_1 are a particular solution of those of Σ_2.

Consider once again (2) expressed as

$$\Sigma_1 :\ \mathbf{x}^{(\alpha)} = \mathbf{f}(\mathbf{x},\mathbf{x},t). \tag{20}$$

Note concretely that in (20), $\mathbf{f}(\mathbf{x},\mathbf{x};t) = \mathbf{f}(\mathbf{x};t)$, that means that this can be separated, depending on the convenience of the result or the design, arbitrarily. Define then an *auxiliary* system in the form

$$\Sigma_2 :\ \chi^{(\alpha)} = \mathbf{f}(\chi,\mathbf{x},t). \tag{21}$$

Clearly, $\chi = \mathbf{x}$ is a particular solution. Then, we can postulate the following theorem:

Theorem 4. Consider the nonlinear commensurate fractional-order system (20) expressed as in (21). If the latter is contractive with respect to χ, then if some solution of χ satisfies a given property (such as smoothness or convergence) in a given region $\mathbf{x} \in \mathcal{X} \subseteq \Re^n$, then all trajectories of the original system (20) verify that given property with asymptotic convergence following a Mittag-Leffler bounding vanishing function, and the original system is said to be partially contractive.

Proof 1. This proof follows the same steps as in Theorem 3 of Lohmiller and Slotine [1998], as the solution of χ-system has a certain particular property, then the particular solution $\chi = \mathbf{x}\,\forall\, t \geq 0$ implies that $\mathbf{x}$ verifies that property asymptotically with a Mittag-Leffler bounding vanishing function.

Following the previous example, the jacobian matrix of Σ_2 is $J(\upsilon) = -1 < 0$, and therefore is partially contracting, so $\lim_{t\to\infty} y(t) \to \upsilon(t)$.

3. SYNCRONIZATION DESIGN VIA CONTRACTION ANALYSIS

From the previous discussion and results on partial contraction, consider that $\Sigma_1 : \mathbf{x}^{(\alpha)} = \mathbf{f}(\mathbf{x}, \mathbf{x}, t)$ is the master system, whose trajectories $\mathbf{x}$ are to be followed by those of a slave system $\Sigma_2 : \hat{\mathbf{x}}^{(\alpha)} = \mathbf{f}(\hat{\mathbf{x}}, \mathbf{x}, t)$. Therefore, if Σ_2 is partially contracting with respect to $\hat{\mathbf{x}}$, then the solutions $\mathbf{x}$ and $\hat{\mathbf{x}}$ converge to each other.

Consider the communication system portrayed in Fig. 1. The basic idea consists of using a chaotic signal generator as a generator of a pseudo-random signal that masks an information signal and delivers it to a secondary system, and the original message can be decoded from the received *contaminated* signal.

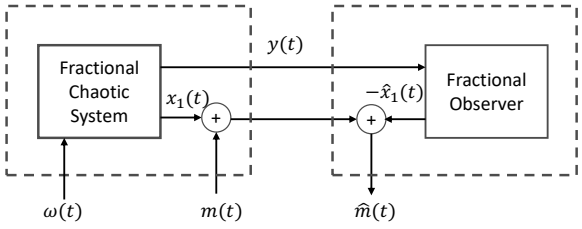

Fig. 1. Communication system using a fractional-order chaotic system and observer

Consider that the first system is given by the Arneodo's chaotic fractional-system

$$\tau \mathbf{x}^{(\alpha)}(t) = \begin{pmatrix} x_2(t) \\ x_3(t) \\ -\beta_1 x_1(t) - \beta_2 x_2(t) - \beta_3 x_3(t) + \beta_4 x_1^3(t) \end{pmatrix} + \omega(t), \quad y(t) = x_1(t), \tag{22}$$

where $\omega(t)$ is a perturbation signal and τ is the time factor. Assuming that only the output $y(t)$ is measured and transmitted, the signal containing the message $m(t)$ is given by

$$y_m(t) = y(t) + m(t) \tag{23}$$

According to Lu [2005], this system shows a chaotic behaviour when $\alpha \in [0.7, 1]$ and $\beta_1 = 5.5$, $\beta_2 = 3.5$, $\beta_3 = 1$ and $\beta_4 = -1$. In this analysis, the time factor can be adjusted in order to create a faster or slower generated chaotic message, and for other values the following results can be adjusted accordingly.

The main problem now is to design an observer that, given that only $y(t)$ is transmitted privately, reconstructs $x(t)$ from $y_m(t)$, given that the former is transmitted over a public channel.

Consider the observer (that receives the synchronization signal $y(t)$), that will work as a *decodifier* for the masked message $m(t)$, given by

$$\tau \hat{\mathbf{x}}^{(\alpha)} = \begin{pmatrix} \hat{x}_2 + K_1(y - \hat{x}_1) \\ \hat{x}_3 + K_2(y - \hat{x}_1) \\ -\beta_1 x_1 - \beta_2 \hat{x}_2 - \beta_3 \hat{x}_3 + \beta_4 x_1^3 + K_3(y - \hat{x}_1) \end{pmatrix}, \tag{24}$$

It is clear that, from the contraction analysis point-of-view, the $\mathbf{x}$ system is a particular solution of $\hat{\mathbf{x}}$ if $\hat{\mathbf{x}} = \mathbf{x}$, $\omega(t) = 0$ and $y = \hat{x}_1$. Therefore, if we can prove that observer is contracting in respect to $\hat{\mathbf{x}}$ then $\lim_{t\to\infty} \hat{\mathbf{x}} = \mathbf{x}$. Taking the Jacobian matrix if the $\hat{\mathbf{x}}$-system we obtain:

$$J_{\hat{\mathbf{x}}} = \begin{pmatrix} -K_1 & 1 & 0 \\ -K_2 & 0 & 1 \\ -K_3 & -\beta_2 & -\beta_3 \end{pmatrix}. \tag{25}$$

In order to search for a gain and parameter combination that assures semi-contraction of system (24), consider the general metric

$$P = \begin{pmatrix} p_1 & p_2 & p_3 \\ p_2 & p_4 & p_5 \\ p_3 & p_5 & p_6 \end{pmatrix}.$$

Solving for a particular metric $P > 0$ such that $\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right)^T P + P\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right) \leq -2\beta_F P$ the synchronization can be achieved.

4. RESULTS

In order to synchronize both systems and symplify the analysis, take $K_1 = K_2 = 0$ and $K_3 > 0$, so the condition for partial contraction is given by the metric

$$P = (P_{c-1} \; P_{c-2} \; P_{c-3})$$

being positive definite, where

$$P_{c-1} = \begin{pmatrix} -\dfrac{4K_3^3 + 4K_3^2 - 10K_3 + 49}{2K_3(2K_3 - 7)} \\ -\dfrac{9K_3^2 + 7}{K_3(2K_3 - 7)} \\ \dfrac{1}{K_3} \end{pmatrix}$$

$$P_{c-2} = \begin{pmatrix} -\dfrac{9K_3^2 + 7}{K_3(2K_3 - 7)} \\ \dfrac{4K_3^2 + 71K_3 + 4}{2\left(7K_3 - 2K_3^2\right)} \\ \dfrac{2\left(K_3^2 + K_3 + 1\right)}{7K_3 - 2K_3^2} \end{pmatrix}$$

$$P_{c-3} = \begin{pmatrix} \dfrac{1}{K_3} \\ \dfrac{2\left(K_3^2 + K_3 + 1\right)}{7K_3 - 2K_3^2} \\ \dfrac{9K_3 + 2}{7K_3 - 2K_3^2} \end{pmatrix}$$

The condition for $P > 0$ is given by $K_3 \in (0, 7/2)$, and according to Theorem 3 the conditions for partial contraction are achieved, so the master and slave systems synchronize $\lim_{t\to\infty} \hat{\mathbf{x}} = \mathbf{x}$.

From the conditions for contraction presented in Section 3, let $K_3 = 1$, so the obtained the metric matrix is

$$P = \begin{pmatrix} 4.7 & 3.2 & 1.0 \\ 3.2 & 7.9 & 1.2 \\ 1.0 & 1.2 & 2.2 \end{pmatrix}.$$

With this result, $\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right)^T P + P\left(\frac{\partial \mathbf{f}}{\partial \mathbf{x}}\right) = -2I_{3\times 3} \leq -\beta_F P < 0$. As the minimum eigenvalue of P is $\lambda_{min}(P) = -1.847$, the condition is met with $\beta_F = 1.0828 > 0$.

Let the message be given by $m(t) = 0.1\sin(2\pi 2t) + 0.05\cos(2\pi 7t)$. In Fig. 2 it is shown the power spectrum of both the masking signal and the message, where it can be seen that the message is effectively masked by the chaotic signal. It should be noted that varying the time scale τ to values different than 1 does modify the bandwidth of the masking signal correspondingly, allowing to different signals to be sent through the channel.

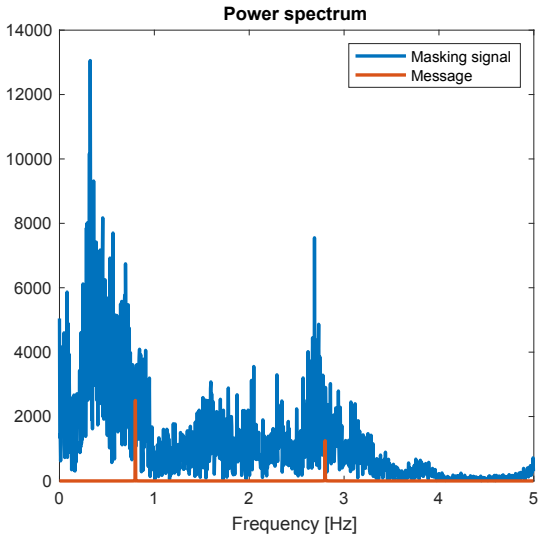

Fig. 2. Power spectrum of the masking signal and message

In Fig. 3 it is depicted the reconstruction of the signal message even under a gaussian perturbation signal $\omega(t)$ with standard deviation $\sigma_\omega = 0.01$ and zero mean. It can be seen of the signal is effectively reconstructed, with a RMS error of 0.0045, that implies a 5% error in reference to the transmitted message.

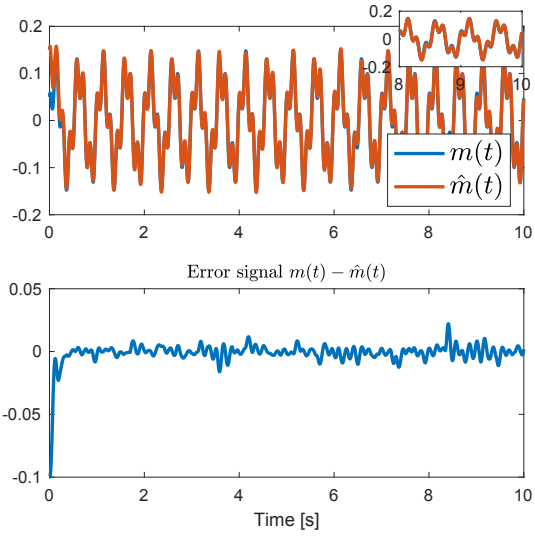

Fig. 3. Signal reconstruction results

5. CONCLUSIONS

This work has presented a contraction analysis-based design for the synchronization of a pair of chaotic fractional order systems that allows to send encrypted information through a channel, using the chaotic sequence generated by a master system as a carrier signal, while a second slave system decrypts the message using a key signal. Contraction analysis provides with a straightforward analysis design, as well as conditions for the synchronization and convergence of neighbor trajectories of both systems. Numeric examples are presented to show the effectiveness of the proposed design. Further work includes the stability and robustness analysis for perturbed and noisy signals recovered from the channel.

6. ACKNOWLEDGEMENTS

Authors want to thank: UACM for its support to this work, UNAM for its support via project PAPIIT-UNAM IN-113418, and CONACyT Project 253677.

REFERENCES

Norelys Aguila-Camacho, Manuel a. Duarte-Mermoud, and Javier a. Gallegos. Lyapunov functions for fractional order systems. *Communications in Nonlinear Science and Numerical Simulation*, 19(9):2951–2957, 2014. ISSN 10075704. doi: 10.1016/j.cnsns.2014.01.022. URL `http://dx.doi.org/10.1016/j.cnsns.2014.01.022`.

Sara Angulo-guzman, Cornelio Posadas-castillo, Miguel Angel Platas-garza, and David Alejandro Diaz-romero. Chaotic Synchronization of Regular and Irregular Complex Networks with Fractional Order Oscillators. *International Journal of Control, Automation and Systems*, 14(4):1114–1123, aug 2016. ISSN 1598-6446. doi: 10.1007/s12555-015-0168-y. URL `http://link.springer.com/ 10.1007/s12555-015-0168-y`.

Riccardo Caponetto. *Fractional order systems: modeling and control applications*, volume 72. World Scientific, 2010.

Michele Caputo. Linear models of dissipation whose q is almost frequency independent-ii. *Geophysical Journal International*, 13(5):529–539, 1967.

E. Delgado and M. A. Duarte. Synchronization of fractional-order systems of the Lorenz type: The non-adaptive case. *IEEE Latin America Transactions*, 12(3):410–415, 2014. ISSN 15480992. doi: 10.1109/TLA.2014.6827866.

Lubomır Dorcák, Vladimir Lesko, and Imrich Kostial. Identification of fractional-order dynamical systems. *arXiv preprint math/0204187*, 2002.

Manuel A Duarte-Mermoud, Norelys Aguila-Camacho, Javier A Gallegos, and Rafael Castro-Linares. Using general quadratic lyapunov functions to prove lyapunov uniform stability for fractional order systems. *Communications in Nonlinear Science and Numerical Simulation*, 22(1):650–659, 2015.

Marcos A González-Olvera and Yu Tang. Contraction analysis for fractional-order nonlinear systems. *Chaos, Solitons & Fractals*, 117:255–263, 2018.

T.T. Hartley, C.F. Lorenzo, and H. Killory Qammer. Chaos in a fractional order Chua's system. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 42(8):485–490, 1995. ISSN 10577122. doi: 10.1109/81.404062. URL `http://ieeexplore.ieee.org/document/404062/`.

Arman Kiani-B, Kia Fallahi, Naser Pariz, and Henry Leung. A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter. *Communications in Nonlinear Science and Numerical Simulation*, 14(3):863–879, 2009. ISSN 10075704. doi: 10.1016/j.cnsns.2007.11.011.

Yan Li, YangQuan Chen, and Igor Podlubny. Mittag-Leffler stability of fractional order nonlinear dynamic systems. *Automatica*, 45(8):1965–1969, 2009. ISSN 00051098. doi: 10.1016/j.automatica.2009.04.003.

Winfried Lohmiller and Jean-Jacques E Slotine. On contraction analysis for non-linear systems. *Automatica*, 34(6):683–696, 1998.

Jun Guo Lu. Chaotic dynamics and synchronization of fractional-order arneodo's systems. *Chaos, Solitons & Fractals*, 26(4):1125–1133, 2005.

Rachid Mansouri, Maamar Bettayeb, and Said Djennoune. Approximation of high order integer systems by fractional order reduced-parameters models. *Mathematical and Computer Modelling*, 51(1-2):53–62, 2010.

Gerardo Navarro-Guerrero and Yu Tang. Fractional order model reference adaptive control for anesthesia. *International Journal of Adaptive Control and Signal Processing*, (January):1–11, 2017. ISSN 08906327. doi: 10.1002/acs.2769. URL `http://doi.wiley.com/10.1002/acs.2769`.

A Oustaloup, P Melchior, P Lanusse, O Cois, and F Dancla. The crone toolbox for matlab. In *CACSD. Conference Proceedings. IEEE International Symposium on Computer-Aided Control System Design (Cat. No. 00TH8537)*, pages 190–195. IEEE, 2000.

Hao Zhu, Shangbo Zhou, and Jun Zhang. Chaos and synchronization of the fractional-order Chua's system. *Chaos, Solitons and Fractals*, 39(4):1595–1603, 2009. ISSN 09600779. doi: 10.1016/j.chaos.2007.06.082. URL `http://dx.doi.org/10.1016/j.chaos.2007.06.082`.

